

PCT/JPO/06308

日本国特許庁

PATENT OFFICE
JAPANESE GOVERNMENT

14.09.00

JPO0/6308

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日

Date of Application:

1999年 9月17日

REC'D 06 NOV 2000

WIPO

PCT

出願番号

Application Number:

平成11年特許願第309722号

EKU

出願人

Applicant(s):

ソニー株式会社

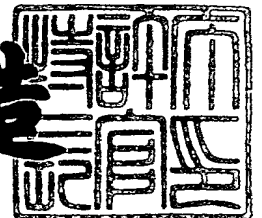
PRIORITY
DOCUMENT

SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH RULE 17.1(a) OR (b)

2000年10月20日

特許庁長官
Commissioner,
Patent Office

及川耕造



出証番号 出証特2000-3085431

【書類名】 特許願
 【整理番号】 9900699277
 【提出日】 平成11年 9月17日
 【あて先】 特許庁長官殿
 【国際特許分類】 H04L 12/16
 【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
 内

【氏名】 野中 聡

【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
 内

【氏名】 江崎 正

【特許出願人】

【識別番号】 000002185

【氏名又は名称】 ソニー株式会社

【代表者】 出井 伸之

【代理人】

【識別番号】 100094053

【弁理士】

【氏名又は名称】 佐藤 隆久

【手数料の表示】

【予納台帳番号】 014890

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9707389

【プルーフの要否】

要

【書類名】 明細書

【発明の名称】 データ提供システムおよびその方法、データ提供装置およびデータ処理装置

【特許請求の範囲】

【請求項 1】

データ提供装置からデータ処理装置にコンテンツデータを配給するデータ提供システムにおいて、

前記データ提供装置は、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する

データ提供システム。

【請求項 2】

前記データ提供装置は、

前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データのうち少なくとも一つのデータの作成者および送信者の正当性を検証するための署名データをさらに格納した前記モジュールを前記データ処理装置に配給する

請求項 1 に記載のデータ提供システム。

【請求項 3】

前記データ提供装置は、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データのうち少なくとも一つのデータについて、当該データが改竄されていないかを検証するためのデータと、当該データを所定の機関によって正規に認証されているかを検証するための署名データとのうち少なくとも一方のデータをさらに格納した前記モジュールを前記データ処理装置に配給する

請求項 2 に記載のデータ提供システム。

【請求項 4】

前記データ処理装置は、前記権利書データに基づいて、前記コンテンツデータの購入形態を決定し、

前記コンテンツデータを他のデータ処理装置に転送する場合に、当該コンテンツデータの購入者の正当性を示す署名データと、当該コンテンツデータの送信者の正当性を示す署名データとを異ならせる

請求項 2 に記載のデータ提供システム。

【請求項 5】

前記データ提供装置は、当該データ提供装置の秘密鍵データおよびハッシュ関数を用いて前記署名データを作成する

請求項 2 に記載のデータ提供システム。

【請求項 6】

データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムにおいて、

前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、

前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとを格納したモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する

データ提供システム。

【請求項 7】

前記管理装置は、前記キーファイルの作成者の正当性を検証するための署名データを生成し、当該署名データをさらに格納した前記キーファイルを作成する

請求項 6 に記載のデータ提供システム。

【請求項 8】

前記データ提供装置は、前記コンテンツ鍵データおよび前記権利書データを生成して前記管理装置に送信し、

前記管理装置は、受信した前記コンテンツ鍵データおよび前記権利書データに基づいて前記キーファイルを作成し、当該作成したキーファイルを登録する

請求項 6 に記載のデータ提供システム。

【請求項 9】

前記データ提供装置は、前記コンテンツファイルの作成者および配給者と、前記キーファイルの配給者との正当性のうち少なくとも一つを検証するための署名データをそれぞれ作成し、当該署名データをさらに格納した前記モジュールを前記データ処理装置に配給する

請求項 7 に記載のデータ提供システム。

【請求項 10】

前記データ処理装置は、前記モジュールに格納された前記署名データを検証して、前記コンテンツファイルの作成者および配給者と、前記キーファイルの作成者および配給者との正当性のうち少なくとも一つを確認する

請求項 9 に記載のデータ提供システム。

【請求項 11】

前記データ提供装置は、前記コンテンツデータが圧縮されている場合に、当該コンテンツデータを伸長する伸長用ソフトウェアを前記コンテンツファイルにさらに格納する

請求項 6 に記載のデータ提供システム。

【請求項 12】

前記データ提供装置は、前記コンテンツファイルに電子透かし情報が埋め込まれている場合に、当該電子透かし情報を検出するのに用いられる情報を含む電子透かし情報モジュールを前記コンテンツファイルにさらに格納する

請求項 6 に記載のデータ提供システム。

【請求項 13】

前記データ提供装置は、前記コンテンツデータの内容の説明に関するメタデータを前記コンテンツファイルに格納して、あるいは前記コンテンツファイルとは別に前記データ処理装置に配給する

請求項 6 に記載のデータ提供システム。

【請求項 14】

前記管理装置は、配信用鍵データを用いて暗号化した前記コンテンツ鍵データおよび前記権利書データを格納した前記キーファイルを作成し、

前記配信用鍵データを前記データ処理装置に配給する

請求項 6 に記載のデータ提供システム。

【請求項 15】

前記管理装置および前記データ処理装置は、有効期間が規定された複数の配信用鍵データを有し、対応する期間の前記配信用鍵データを用いる

請求項 14 に記載のデータ提供システム。

【請求項 16】

前記管理装置は、前記権利書データの文法を記述したデータをさらに格納した前記キーファイルを作成する

請求項 6 に記載のデータ提供システム。

【請求項 17】

前記管理装置は、前記コンテンツファイルおよび前記キーファイルを読み込むための情報を示すデータであるファイルリーダーを前記データ処理装置に配給し、

前記データ処理装置は、前記ファイルリーダーに基づいて、前記コンテンツファイルおよび前記キーファイルの読み込みを行う

請求項 6 に記載のデータ提供システム。

【請求項 18】

前記データ提供装置は、前記コンテンツファイルおよび前記キーファイルを読み込むための情報を示すデータであるファイルリーダーをさらに格納した前記モジュールを前記データ処理装置に配給し、

前記データ処理装置は、前記ファイルリーダーに基づいて、前記コンテンツファイルおよび前記キーファイルの読み込みを行う

請求項 6 に記載のデータ提供システム。

【請求項 19】

前記データ提供装置は、自らの秘密鍵データを用いて前記署名データを作成し

、
前記データ処理装置は、前記秘密鍵データに対応する公開鍵データを用いて、
前記署名データの正当性を検証する

請求項 10 に記載のデータ提供システム。

【請求項 20】

前記データ提供装置は、前記公開鍵データの正当性を証明する公開鍵証明書データをさらに格納した前記モジュールを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた公開鍵証明書データに格納された公開鍵データを用いて前記署名データの検証を行う

請求項 19 に記載のデータ提供システム。

【請求項 21】

前記管理装置は、前記公開鍵データの正当性を証明する公開鍵証明書データを前記データ処理装置に配給する

前記データ処理装置は、前記配給を受けた公開鍵証明書データに格納された公開鍵データを用いて前記署名データの検証を行う

請求項 19 に記載のデータ提供システム。

【請求項 22】

前記データ提供装置は、前記データ処理装置との間で相互認証を行い、当該相互認証によって得たセッション鍵データを用いて前記モジュールを暗号化し、当該暗号化したモジュールを前記データ処理装置に送信する

請求項 6 に記載のデータ提供システム。

【請求項 23】

前記データ提供装置は、前記モジュールを記録した記録媒体を作成する

請求項 6 に記載のデータ提供システム。

【請求項 24】

前記データ処理装置は、前記権利書データに基づいて、前記コンテンツデータ

の購入形態および利用形態の少なくとも一方を決定する

請求項 6 に記載のデータ提供システム。

【請求項 25】

前記データ処理装置は、前記復号したコンテンツ鍵データと、前記暗号化されたコンテンツデータとを復号装置に出力する

請求項 6 に記載のデータ提供システム。

【請求項 26】

前記データ処理装置は、前記権利書データに基づいて、前記配給を受けたコンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の少なくとも一方の履歴を示す履歴データを前記管理装置に送信し、

前記管理装置は、受信した前記履歴データに基づいて、前記データ処理装置における前記コンテンツデータの前記購入および前記利用に伴って得られた利益を、前記データ提供装置の関係者に分配するための利益分配処理を行う

請求項 6 に記載のデータ提供システム。

【請求項 27】

前記管理装置は、コンテンツデータ単位で、前記利益分配処理を行う

請求項 26 に記載のデータ提供システム。

【請求項 28】

前記データ提供装置は、複数の前記コンテンツファイルと、当該複数のコンテンツファイルにそれぞれ対応する複数のキーファイルとを格納したモジュールを前記データ処理装置に配給し、

前記コンテンツファイルには、前記複数のコンテンツファイル相互間の関係と、前記キーファイルとの関係とを示すディレクトリ構造データが含まれている

請求項 6 に記載のデータ提供システム。

【請求項 29】

前記データ提供装置は、

前記モジュールを格納する記憶回路

をさらに有する請求項 6 に記載のデータ提供システム。

【請求項 30】

前記データ提供装置は、
前記コンテンツデータに固有に割り付けられたコンテンツ識別子に基づいて、
前記モジュールを管理する
請求項 29 に記載のデータ提供システム。

【請求項 31】

前記管理装置は、
前記コンテンツ識別子をさらに格納した前記キーファイルを作成する
請求項 30 に記載のデータ提供システム。

【請求項 32】

前記コンテンツ識別子は、
前記データ提供装置が前記記憶回路に格納するコンテンツデータ内でユニーク
に決められている
請求項 30 に記載のデータ提供システム。

【請求項 33】

前記コンテンツ識別子は、
前記グローバルユニークに決められている
請求項 30 に記載のデータ提供システム。

【請求項 34】

前記データ提供装置は、前記コンテンツ識別子を生成する
請求項 30 に記載のデータ提供システム。

【請求項 35】

前記データ提供装置は、
前記モジュールを格納する記憶回路
をさらに有する請求項 30 に記載のデータ提供システム。

【請求項 36】

前記データ処理装置は、その処理内容、内部メモリに記憶された所定のデータ
および処理中のデータを、外部から監視および改竄困難なモジュールを有する
請求項 6 に記載のデータ提供システム。

【請求項 37】

管理装置によって管理され、データ処理装置にコンテンツデータを配給するデータ提供装置において、

暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを前記管理装置から受け、

前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとを格納したモジュールを前記データ処理装置に配給する

データ提供装置。

【請求項 38】

管理装置によって管理され、コンテンツデータを利用するデータ処理装置において、

暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルと、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルとを含むモジュールを受け、

前記権利書データに基づいて、前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の少なくとも一方の履歴を示す履歴データを前記管理装置に送信する

データ処理装置。

【請求項 39】

データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムにおいて、

前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、

前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けたキーファイルとを含むコンテンツファイルを格納したモジュールを、所定の通信プロトコルを用いて当該通信プロトコル

に依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し

、
前記データ処理装置は、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する

データ提供システム。

【請求項 4 0】

データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムにおいて、

前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、

前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して個別に前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供システム。

【請求項 4 1】

前記データ提供装置は、複数の前記コンテンツファイルと、当該複数のコンテンツファイルにそれぞれ対応する複数のキーファイルとを個別に前記データ処理装置に配給し、

前記コンテンツファイルおよび前記キーファイルには、相互間の対応関係を示すハイパーリンク情報が含まれている

請求項 4 0 に記載のデータ提供システム。

【請求項 4 2】

データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムにおいて、

前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に配給し、

前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供システム。

【請求項 4 3】

前記データ提供装置は、複数の前記コンテンツファイルを前記データ処理装置に配給し、

前記管理装置は、前記複数のコンテンツファイルにそれぞれ対応する複数のキーファイルを前記データ処理装置に配給し、

前記コンテンツファイルおよび前記キーファイルには、相互間の対応関係を示すハイパーリンク情報が含まれている

請求項 4 2 に記載のデータ提供システム。

【請求項 4 4】

データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムにおいて、

前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、

前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記キーファイルとを格納したモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する

データ提供システム。

【請求項 45】

データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムにおいて、

前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、

前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記キーファイルとを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して個別に前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツデータの取り扱いを決定する

データ提供システム。

【請求項 46】

データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムにおいて、

前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に配給し、

前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツデータの取り扱いを決定するデータ提供システム。

【請求項 47】

データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムにおいて、

前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを作成し、

前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記暗号化されたコンテンツ鍵データおよび前記暗号化された権利書データとを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して個別に前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定するデータ提供システム。

【請求項 48】

データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムにおいて、

前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを作成して前記データ処理装置に配給し、

前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツデータの取り扱いを決定する

データ提供システム。

【請求項 4 9】

データ提供装置、データ配給装置およびデータ処理装置を有するデータ提供システムにおいて、

前記データ提供装置は、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納した第 1 のモジュールを前記データ配給装置に提供し、

前記データ配給装置は、前記提供を受けた前記第 1 のモジュールに格納された前記暗号化されたコンテンツデータ、コンテンツ鍵データおよび権利書データを格納した第 2 のモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記第 2 のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する

データ提供システム。

【請求項 5 0】

前記データ配給装置は、前記提供を受けた第 1 のモジュールを包括させた前記第 2 のモジュールを作成し、当該作成した第 2 のモジュールを前記データ処理装置に配給する

請求項 4 9 に記載のデータ提供システム。

【請求項 5 1】

前記データ配給装置は、前記コンテンツデータの価格を示す価格データをさらに格納した前記第 2 のモジュールを前記データ処理装置に配給する

請求項 4 9 に記載のデータ提供システム。

【請求項 5 2】

前記データ配給装置は、前記データ提供装置が前記コンテンツデータについて決定した卸売価格に基づいて、前記価格データを決定する

請求項 5 1 に記載のデータ提供システム。

【請求項 5 3】

前記データ提供装置は、

前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データのうち少なくとも一つのデータの作成者および送信者の正当性を検証するための署名データをさらに格納した前記第 1 のモジュールを前記データ配給装置に提供する

請求項 4 9 に記載のデータ提供システム。

【請求項 5 4】

前記データ提供装置は、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データのうち少なくとも一つのデータについて、当該データが改竄されていないかを検証するためのデータと、当該データを所定の機関によって正規に認証されているかを検証するための署名データとのうち少なくとも一方のデータをさらに格納した前記第 1 のモジュールを前記データ配給装置に提供する

請求項 5 3 に記載のデータ提供システム。

【請求項 5 5】

前記データ配給装置は、

前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データのうち少なくとも一つのデータの作成者および送信者の正当性を検証するための署名データをさらに格納した前記第 2 のモジュールを前記データ処理装置に提供する

請求項 4 9 に記載のデータ提供システム。

【請求項 5 6】

前記データ配給装置は、

前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データのう

ち少なくとも一つのデータについて、当該データが改竄されていないかを検証するためのデータと、当該データを所定の機関によって正規に認証されているかを検証するための署名データとのうち少なくとも一方のデータをさらに格納した前記第2のモジュールを前記データ処理装置に提供する

請求項49に記載のデータ提供システム。

【請求項57】

管理装置をさらに有し、

前記データ処理装置は、前記権利書データに基づいて、前記配給を受けたコンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の少なくとも一方の履歴を示す履歴データを前記管理装置に送信し、

前記管理装置は、受信した前記履歴データに基づいて、前記データ処理装置における前記コンテンツデータの前記購入および前記利用に伴って得られた利益を、前記データ提供装置および前記データ配給装置の関係者に分配するための利益分配処理を行う

請求項49に記載のデータ提供システム。

【請求項58】

前記データ処理装置は、前記データ配給装置の前記配給に関しての配給用履歴データを前記データ配給装置に送信し、

前記データ配給装置は、前記配給用履歴データに基づいて、前記配給に関しての課金処理を行う

請求項49に記載のデータ提供システム。

【請求項59】

データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供システムにおいて、

前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、

前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとを格納した第1のモジュールを前記データ配給装置に提供し、

前記データ配給装置は、前記提供を受けたコンテンツファイルおよび前記キーファイルを格納した第2のモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記第2のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記第2のモジュールに格納された前記コンテンツデータの取り扱いを決定する

データ提供システム。

【請求項60】

前記管理装置は、前記キーファイルの作成者の正当性を検証するための署名データを生成し、当該署名データをさらに格納した前記キーファイルを作成する
請求項59に記載のデータ提供システム。

【請求項61】

前記データ提供装置は、前記コンテンツ鍵データおよび前記権利書データを生成して前記管理装置に送信し、

前記管理装置は、受信した前記コンテンツ鍵データおよび前記権利書データに基づいて前記キーファイルを作成し、前記受信した前記コンテンツ鍵データおよび前記権利書データを登録する

請求項59に記載のデータ提供システム。

【請求項62】

前記データ提供装置は、前記コンテンツファイルの作成者および提供者と、前記キーファイルの提供者との正当性のうち少なくとも一つを検証するための署名データをそれぞれ作成し、当該署名データをさらに格納した前記第1のモジュールを前記データ処理装置に配給する

請求項59に記載のデータ提供システム。

【請求項 63】

前記データ配給装置は、前記コンテンツファイルの作成者および配給者と、前記キーファイルの配給者との正当性のうち少なくとも一つを検証するための署名データをそれぞれ作成し、当該署名データをさらに格納した前記第2のモジュールを前記データ処理装置に配給する

請求項 59 に記載のデータ提供システム。

【請求項 64】

前記データ処理装置は、前記第2のモジュールに格納された前記署名データを検証して、前記コンテンツファイルの作成者および配給者と、前記キーファイルの作成者および配給者との正当性のうち少なくとも一つを確認する

請求項 63 に記載のデータ提供システム。

【請求項 65】

前記データ提供装置は、前記コンテンツデータが圧縮されている場合に、当該コンテンツデータを伸長する伸長用ソフトウェアを前記コンテンツファイルにさらに格納する

請求項 59 に記載のデータ提供システム。

【請求項 66】

前記データ提供装置は、前記コンテンツデータの内容の説明に関するメタデータを前記コンテンツファイルに格納して、あるいは前記コンテンツファイルとは別に前記データ配給装置に配給する

請求項 59 に記載のデータ提供システム。

【請求項 67】

前記データ提供装置は、前記コンテンツファイルに電子透かし情報が埋め込まれている場合に、当該電子透かし情報を検出するのに用いられる情報を含む電子透かし情報モジュールを前記コンテンツファイルにさらに格納する

請求項 59 に記載のデータ提供システム。

【請求項 68】

前記管理装置は、配信用鍵データを用いて暗号化した前記コンテンツ鍵データおよび前記権利書データを格納した前記キーファイルを作成し、

前記配信用鍵データを前記データ処理装置に配給する

請求項 59 に記載のデータ提供システム。

【請求項 69】

前記管理装置および前記データ処理装置は、有効期間が規定された複数の配信用鍵データを有し、対応する期間の前記配信用鍵データを用いる

請求項 68 に記載のデータ提供システム。

【請求項 70】

前記管理装置は、前記権利書データの文法を記述したデータをさらに格納した前記キーファイルを作成する

請求項 59 に記載のデータ提供システム。

【請求項 71】

前記管理装置は、前記コンテンツファイルおよび前記キーファイルを読み込むための情報を示すデータであるファイルリーダーを前記データ処理装置に配給し、

前記データ処理装置は、前記ファイルリーダーに基づいて、前記コンテンツファイルおよび前記キーファイルの読み込みを行う

請求項 59 に記載のデータ提供システム。

【請求項 72】

前記データ提供装置は、前記コンテンツファイルおよび前記キーファイルを読み込むための情報を示すデータであるファイルリーダーをさらに格納した前記モジュールを前記データ処理装置に配給し、

前記データ処理装置は、前記ファイルリーダーに基づいて、前記コンテンツファイルおよび前記キーファイルの読み込みを行う

請求項 59 に記載のデータ提供システム。

【請求項 73】

前記データ提供装置は、自らの秘密鍵データを用いて前記署名データを作成し、

前記データ処理装置は、前記秘密鍵データに対応する公開鍵データを用いて、前記署名データの正当性を検証する

請求項 62 に記載のデータ提供システム。

【請求項 7 4】

前記データ提供装置は、前記公開鍵データの正当性を証明する公開鍵証明書データをさらに格納した前記モジュールを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた公開鍵証明書データに格納された公開鍵データを用いて前記署名データの検証を行う

請求項 7 3 に記載のデータ提供システム。

【請求項 7 5】

前記管理装置は、前記公開鍵データの正当性を証明する公開鍵証明書データを前記データ処理装置に配給する

前記データ処理装置は、前記配給を受けた公開鍵証明書データに格納された公開鍵データを用いて前記署名データの検証を行う

請求項 7 3 に記載のデータ提供システム。

【請求項 7 6】

前記データ配給装置は、自らの秘密鍵データを用いて前記署名データを作成し、

前記データ処理装置は、前記秘密鍵データに対応する公開鍵データを用いて、前記署名データの正当性を検証する

請求項 6 3 に記載のデータ提供システム。

【請求項 7 7】

前記データ配給装置は、前記公開鍵データの正当性を証明する公開鍵証明書データをさらに格納した前記モジュールを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた公開鍵証明書データに格納された公開鍵データを用いて前記署名データの検証を行う

請求項 7 6 に記載のデータ提供システム。

【請求項 7 8】

前記管理装置は、前記公開鍵データの正当性を証明する公開鍵証明書データを前記データ処理装置に配給する

前記データ処理装置は、前記配給を受けた公開鍵証明書データに格納された公開鍵データを用いて前記署名データの検証を行う

請求項 7 6 に記載のデータ提供システム。

【請求項 7 9】

前記データ配給装置は、前記データ処理装置との間で相互認証を行い、当該相互認証によって得たセッション鍵データを用いて前記モジュールを暗号化し、当該暗号化した前記第 2 のモジュールを前記データ処理装置に送信する

請求項 5 9 に記載のデータ提供システム。

【請求項 8 0】

前記データ配給装置は、前記モジュールを記録した記録媒体を作成する
請求項 5 0 に記載のデータ提供システム。

【請求項 8 1】

前記データ処理装置は、前記権利書データに基づいて、前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定する
請求項 5 9 に記載のデータ提供システム。

【請求項 8 2】

前記データ処理装置は、前記復号したコンテンツ鍵データと、前記暗号化されたコンテンツデータとを復号装置に出力する
請求項 5 9 に記載のデータ提供システム。

【請求項 8 3】

前記データ処理装置は、前記権利書データに基づいて、前記配給を受けたコンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の少なくとも一方の履歴を示す履歴データを前記管理装置に送信し、

前記管理装置は、受信した前記履歴データに基づいて、前記データ処理装置における前記コンテンツデータの前記購入および前記利用に伴って得られた利益を、前記データ提供装置および前記データ配給装置の関係者に分配するための利益分配処理を行う

請求項 5 9 に記載のデータ提供システム。

【請求項 8 4】

前記管理装置は、コンテンツデータ単位で、前記利益分配処理を行う

請求項 8 3 に記載のデータ提供システム。

【請求項 8 5】

前記データ配給装置は、前記コンテンツデータの価格を示す価格データを格納した前記第 2 のモジュールを前記データ処理装置に配給する

請求項 5 9 に記載のデータ提供システム。

【請求項 8 6】

前記管理装置は、前記データ配給装置から受けた前記価格データを登録する
請求項 8 5 に記載のデータ提供システム。

【請求項 8 7】

前記データ処理装置は、その処理内容、内部メモリに記憶された所定のデータおよび処理中のデータを、外部から監視および改竄困難なモジュールを有する

請求項 5 9 に記載のデータ提供システム。

【請求項 8 8】

前記第 1 のモジュールおよび前記第 2 のモジュールに、複数のコンテンツファイルと、当該複数のコンテンツファイルに対応する複数のキーファイルとが格納されている場合に、

前記第 1 のモジュールおよび前記第 2 のモジュールには、それぞれ前記複数のコンテンツファイルと、それらに対応するキーファイルとの対応関係を示すデータがさらに含まれている

請求項 5 9 に記載のデータ提供システム。

【請求項 8 9】

前記データ提供装置は、複数の前記コンテンツファイルと、当該複数のコンテンツファイルにそれぞれ対応する複数のキーファイルとを格納したモジュールを前記データ処理装置に配給し、

前記コンテンツファイルには、前記複数のコンテンツファイル相互間の関係と、前記キーファイルとの関係とを示すディレクトリ構造データが含まれている

請求項 5 9 に記載のデータ提供システム。

【請求項 9 0】

前記データ提供装置は、

前記モジュールを格納する記憶回路

をさらに有する請求項 59 に記載のデータ提供システム。

【請求項 91】

前記データ提供装置は、

前記コンテンツデータに固有に割り付けられたコンテンツ識別子に基づいて、

前記モジュールを管理する

請求項 90 に記載のデータ提供システム。

【請求項 92】

前記管理装置は、

前記コンテンツ識別子をさらに格納した前記キーファイルを作成する

請求項 91 に記載のデータ提供システム。

【請求項 93】

前記コンテンツ識別子は、

前記データ提供装置が前記記憶回路に格納するコンテンツデータ内でユニーク
に決められている

請求項 91 に記載のデータ提供システム。

【請求項 94】

前記コンテンツ識別子は、

前記グローバルユニークに決められている

請求項 91 に記載のデータ提供システム。

【請求項 95】

前記データ提供装置は、前記コンテンツ識別子を生成する

請求項 91 に記載のデータ提供システム。

【請求項 96】

前記データ提供装置は、

前記モジュールを格納する記憶回路

をさらに有する請求項 91 に記載のデータ提供システム。

【請求項 97】

データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ

配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供システムにおいて、

前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、

前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと前記管理装置から受けたキーファイルとを含むコンテンツファイルを格納した第1のモジュールを前記データ配給装置に提供し、

前記データ配給装置は、前記提供を受けたコンテンツファイルを格納した第2のモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記第2のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記第2のモジュールに格納された前記コンテンツデータの取り扱いを決定する

データ提供システム。

【請求項98】

データ提供装置から第1のデータ配給装置および第2のデータ配給装置にコンテンツデータを提供し、前記第1のデータ配給装置および前記第2のデータ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記第1のデータ配給装置、前記第2のデータ配給装置および前記データ処理装置を管理するデータ提供システムにおいて、

前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、

前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとを格納した第1のモジュールを前記第1のデータ配給装置および前記第2のデータ配給装置に提供し、

前記第1のデータ配給装置は、前記提供を受けたコンテンツファイルおよび前

記キーファイルを格納した第 2 のモジュールを前記データ処理装置に配給し、

前記第 2 のデータ配給装置は、前記提供を受けたコンテンツファイルおよび前記キーファイルを格納した第 3 のモジュールを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記第 2 のモジュールおよび前記第 3 のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する

データ提供システム。

【請求項 9 9】

前記第 1 のデータ配給装置は、前記コンテンツデータの価格を示す第 1 の価格データを格納した前記第 2 のモジュールを前記データ処理装置に配給し、

前記第 2 のデータ配給装置は、前記コンテンツデータの価格を示す第 2 の価格データを格納した前記第 3 のモジュールを前記データ処理装置に配給し、

請求項 9 6 に記載のデータ提供システム。

【請求項 1 0 0】

第 1 のデータ提供装置からデータ配給装置に第 1 のコンテンツデータを提供し、第 2 のデータ提供装置からデータ配給装置に第 2 のコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記第 1 のデータ提供装置、前記第 2 のデータ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供システムにおいて、

前記管理装置は、暗号化された第 1 のコンテンツ鍵データと前記第 1 のコンテンツデータの取り扱いを示す暗号化された第 1 の権利書データとを格納した第 1 のキーファイルと、暗号化された第 2 のコンテンツ鍵データと前記第 2 のコンテンツデータの取り扱いを示す暗号化された第 2 の権利書データとを格納した第 2 のキーファイルとを作成し、

前記第 1 のデータ提供装置は、前記第 1 のコンテンツ鍵データを用いて暗号化された前記第 1 のコンテンツデータを格納した第 1 のコンテンツファイルと、前記管理装置から受けた前記第 1 のキーファイルとを格納した第 1 のモジュールを前記データ配給装置に提供し、

前記第2のデータ提供装置は、前記第2のコンテンツ鍵データを用いて暗号化された前記第2のコンテンツデータを格納した第2のコンテンツファイルと、前記管理装置から受けた前記第2のキーファイルとを格納した第2のモジュールを前記データ配給装置に提供し、

前記データ配給装置は、前記提供を受けた前記第1のコンテンツファイル、前記第1のキーファイル、前記第2のコンテンツファイルおよび前記第2のキーファイルを格納した第3のモジュールを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記第3のモジュールに格納された前記第1のコンテンツ鍵データ、前記第2のコンテンツ鍵データ、前記第1の権利書データおよび前記第2の権利書データを復号し、当該復号した第1の権利書データに基づいて前記第1のコンテンツデータの取り扱いを決定し、前記復号した第2の権利書データに基づいて前記第2のコンテンツデータの取り扱いを決定する

データ提供システム。

【請求項101】

前記データ配給装置は、前記第1のコンテンツデータの価格を示す第1の価格データと、前記第2のコンテンツデータの価格を示す第2の価格データとをさらに格納した前記第3のモジュールを前記データ処理装置に配給する

請求項98に記載のデータ提供システム。

【請求項102】

データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供システムにおいて、

前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、

前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとを個別に前記データ配給装置に配給し、

前記データ配給装置は、配給を受けた前記コンテンツファイルと前記キーファイルとを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して個別に前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供システム。

【請求項 103】

前記コンテンツファイルおよび前記キーファイルには、相互間の対応関係を明示するためのデータが含まれる

請求項 102 に記載のデータ提供システム。

【請求項 104】

データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムにおいて、

前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に配給し、

前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルを前記データ配給装置に提供し、

前記データ配給装置は、前記提供を受けたコンテンツファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供システム。

【請求項 105】

前記コンテンツファイルおよび前記キーファイルには、相互間の対応関係を明示するためのデータが含まれる

請求項 104 に記載のデータ提供システム。

【請求項 106】

データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供システムにおいて、

前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、

前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記キーファイルとを格納した第 1 のモジュールを前記データ配給装置に提供し、

前記データ配給装置は、前記提供を受けたコンテンツデータおよび前記キーファイルを格納した第 2 のモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記第 2 のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記第 2 のモジュールに格納された前記コンテンツデータの取り扱いを決定する

データ提供システム。

【請求項 107】

データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供システムにおいて、

前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの

取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、

前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記キーファイルとを個別に前記データ配給装置に配給し、

前記データ配給装置は、配給を受けた前記コンテンツデータと前記キーファイルとを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して個別に前記データ配給装置に配給し、

前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツデータの取り扱いを決定する

データ提供システム。

【請求項 108】

データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムにおいて、

前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に配給し、

前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを前記データ配給装置に提供し、

前記データ配給装置は、前記提供を受けたコンテンツデータを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツデータの取り扱いを決定する

データ提供システム。

【請求項 109】

データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ

配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供システムにおいて、

前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを前記データ提供装置に提供し、

前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記暗号化されたコンテンツ鍵データおよび前記暗号化された権利書データとを個別に前記データ配給装置に配給し、

前記データ配給装置は、配給を受けた前記コンテンツデータと前記暗号化されたコンテンツ鍵データおよび前記暗号化された権利書データとを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して個別に前記データ配給装置に配給し、

前記データ処理装置は、前記配給を受けた前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツデータの取り扱いを決定する

データ提供システム。

【請求項 110】

データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供システムにおいて、

前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを前記データ処理装置に配給し、

前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを前記データ配給装置に提供し、

前記データ配給装置は、前記提供を受けたコンテンツデータを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記コンテンツ鍵データおよび前記

権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツデータの取り扱いを決定する

データ提供システム。

【請求項 111】

データ提供装置、データ配給装置、管理装置およびデータ処理装置を有するデータ提供システムにおいて、

前記データ提供装置は、コンテンツのマスタソースデータを前記管理装置に提供し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置を管理し、前記提供されたマスタソースデータをコンテンツ鍵データを用いて暗号化してコンテンツデータを作成し、当該コンテンツデータを格納したコンテンツファイルを作成し、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記コンテンツファイルおよび前記キーファイルを前記データ配給装置に提供し、

前記データ配給装置は、前記提供を受けた前記コンテンツファイルおよび前記キーファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供システム。

【請求項 112】

前記管理装置は、前記コンテンツファイルおよび前記キーファイルを格納した第1のモジュールを作成し、当該第1のモジュールを前記データ配給装置に提供し、

前記データ配給装置は、前記第1のモジュールに格納された前記コンテンツファイルおよび前記キーファイルを格納した第2のモジュールを生成し、当該第2

のモジュールを前記データ処理装置に配給する

請求項 111 に記載のデータ提供システム。

【請求項 113】

前記管理装置は、前記コンテンツファイルを記憶および管理するデータベース、前記キーファイルを記憶および管理するデータベース、および前記権利書データを記憶および管理するデータベースのうち、少なくとも一つのデータベースを有し、

前記コンテンツデータに固有に割り当てられたコンテンツ識別子を用いて、前記コンテンツファイル、前記キーファイルおよび前記権利書データの少なくとも一つを一元的に管理する

請求項 111 に記載のデータ提供システム。

【請求項 114】

前記データ提供装置は、

前記コンテンツ鍵データおよび前記権利書データを前記管理装置に提供する

請求項 111 に記載のデータ提供システム。

【請求項 115】

データ提供装置、データ配給装置、管理装置およびデータ処理装置を有するデータ提供システムにおいて、

前記データ提供装置は、コンテンツのマスタソースデータを前記管理装置に提供し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置を管理し、前記提供されたマスタソースデータをコンテンツ鍵データを用いて暗号化してコンテンツデータを作成し、当該コンテンツデータを格納したコンテンツファイルを作成し、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記コンテンツファイルを前記データ配給装置に提供し、前記キーファイルを前記データ処理装置に提供し、

前記データ配給装置は、前記提供を受けた前記コンテンツファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録

媒体に記録して前記データ処理装置に配給し、

前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供システム。

【請求項 116】

データ提供装置、データ配給装置、管理装置およびデータ処理装置を有するデータ提供システムにおいて、

前記データ提供装置は、コンテンツ鍵データを用いた暗号化したコンテンツデータを格納したコンテンツファイルを前記管理装置に提供し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置を管理し、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置から提供を受けた前記コンテンツファイルと、前記作成したキーファイルとを前記データ配給装置に提供し、

前記データ配給装置は、前記提供を受けた前記コンテンツファイルおよび前記キーファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供システム。

【請求項 117】

前記管理装置は、前記コンテンツファイルおよび前記キーファイルを格納した第1のモジュールを作成し、当該第1のモジュールを前記データ配給装置に提供し、

前記データ配給装置は、前記第1のモジュールに格納された前記コンテンツフ

ファイルおよび前記キーファイルを格納した第2のモジュールを生成し、当該第2のモジュールを前記データ処理装置に配給する

請求項 116 に記載のデータ提供システム。

【請求項 118】

前記管理装置は、前記コンテンツファイルを記憶および管理するデータベース、前記キーファイルを記憶および管理するデータベース、および前記権利書データを記憶および管理するデータベースのうち、少なくとも一つのデータベースを有し、

前記コンテンツデータに固有に割り当てられたコンテンツ識別子を用いて、前記コンテンツファイル、前記キーファイルおよび前記権利書データの少なくとも一つを一元的に管理する

請求項 116 に記載のデータ提供システム。

【請求項 119】

前記データ提供装置は、

前記コンテンツ鍵データおよび前記権利書データを前記管理装置に提供する

請求項 114 に記載のデータ提供システム。

【請求項 120】

データ提供装置、データ配給装置、管理装置およびデータ処理装置を有するデータ提供システムにおいて、

前記データ提供装置は、コンテンツ鍵データを用いた暗号化したコンテンツデータを格納したコンテンツファイルを前記管理装置に提供し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置を管理し、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置から提供を受けた前記コンテンツファイルを前記データ配給装置に提供し、前記作成したキーファイルを前記データ処理装置に提供し、

前記データ配給装置は、前記提供を受けた前記コンテンツファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録

媒体に記録して前記データ処理装置に配給し、

前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供システム。

【請求項 121】

データ提供装置、データ配給装置、管理装置、データベース装置およびデータ処理装置を有するデータ提供システムにおいて、

前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルおよび前記管理装置から提供を受けたキーファイルを前記データベース装置に格納し、

前記管理装置は、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ提供装置に提供し、

前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルおよびキーファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供システム。

【請求項 122】

前記データベース装置は、前記コンテンツデータに固有に割り当てられたコンテンツ識別子を用いて、前記格納しているコンテンツファイルおよびキーファイルを一元的に管理する

請求項 121 に記載のデータ提供システム。

【請求項 1 2 3】

前記管理装置は、前記キーファイルを記憶および管理するデータベース、および前記権利書データを記憶および管理するデータベースのうち、少なくとも一つのデータベースを有し、

前記コンテンツデータに固有に割り当てられたコンテンツ識別子を用いて、前記キーファイルおよび前記権利書データの少なくとも一つを一元的に管理する

請求項 1 2 1 に記載のデータ提供システム。

【請求項 1 2 4】

前記データ提供装置は、

前記コンテンツ鍵データおよび前記権利書データを前記管理装置に提供する

請求項 1 2 1 に記載のデータ提供システム。

【請求項 1 2 5】

データ提供装置、データ配給装置、管理装置、データベース装置およびデータ処理装置を有するデータ提供システムにおいて、

前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データベース装置に格納し、

前記管理装置は、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ配給装置に提供し、

前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルと、前記データ配給装置から提供を受けたキーファイルとを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供システム。

【請求項 1 2 6】

データ提供装置、データ配給装置、管理装置、データベース装置およびデータ処理装置を有するデータ提供システムにおいて、

前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データベース装置に格納し、

前記管理装置は、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に提供し、

前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供システム。

【請求項 1 2.7】

複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を有するデータ提供システムにおいて、

前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルおよび対応する前記管理装置から提供を受けたキーファイルを前記データベース装置に格納し、

前記管理装置は、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルに対応する前記データ提供装置に提供し、

前記データ配給装置は、前記データベース装置から得た前記コンテンツファイ

ルおよびキーファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供システム。

【請求項 128】

前記データベース装置は、前記コンテンツデータに固有に割り当てられたコンテンツ識別子を用いて、前記格納しているコンテンツファイルおよびキーファイルを一元的に管理する

請求項 127 に記載のデータ提供システム。

【請求項 129】

前記管理装置は、前記キーファイルを記憶および管理するデータベース、および前記権利書データを記憶および管理するデータベースのうち、少なくとも一つのデータベースを有し、

対応するデータ提供装置において、当該データ提供装置が提供する前記コンテンツデータに固有に割り当てられたコンテンツ識別子を用いて、前記キーファイルおよび前記権利書データの少なくとも一つを一元的に管理する

請求項 127 に記載のデータ提供システム。

【請求項 130】

前記データ提供装置は、

前記コンテンツ鍵データおよび前記権利書データを前記管理装置に提供する

請求項 127 に記載のデータ提供システム。

【請求項 131】

複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を有するデータ提供システムにおいて、

前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し

、当該作成したコンテンツファイルを前記データベース装置に格納し、

前記管理装置は、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ配給装置に提供し、

前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルと、前記管理装置から提供を受けたキーファイルとを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供システム。

【請求項 1 3 2】

複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を有するデータ提供システムにおいて、

前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データベース装置に格納し、

前記管理装置は、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に提供し、

前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書デー

タに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供システム。

【請求項 133】

複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を有するデータ提供システムにおいて、

前記データ提供装置は、コンテンツデータのマスソースを対応する前記管理装置に提供し、当該管理装置から受けたコンテンツファイルおよびキーファイルを前記データベースに格納し、

前記管理装置は、対応する前記データ提供装置から受けた前記マスソースをコンテンツ鍵データを用いて暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記作成したコンテンツファイルおよび前記作成したキーファイルを対応する前記データ提供装置に送り、

前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルおよびキーファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供システム。

【請求項 134】

前記データベース装置は、前記コンテンツデータに固有に割り当てられたコンテンツ識別子を用いて、前記格納しているコンテンツファイルおよびキーファイルを一元的に管理する

請求項 133 に記載のデータ提供システム。

【請求項 135】

前記管理装置は、前記キーファイルを記憶および管理するデータベース、および前記権利書データを記憶および管理するデータベースのうち、少なくとも一つのデータベースを有し、

対応するデータ提供装置において、当該データ提供装置が提供する前記コンテンツデータに固有に割り当てられたコンテンツ識別子を用いて、前記キーファイルおよび前記権利書データの少なくとも一つを一元的に管理する

請求項 133 に記載のデータ提供システム。

【請求項 136】

前記データ提供装置は、

前記コンテンツ鍵データおよび前記権利書データを前記管理装置に提供する

請求項 133 に記載のデータ提供システム。

【請求項 137】

複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を有するデータ提供システムにおいて、

前記データ提供装置は、コンテンツデータのマスソースを対応する前記管理装置に提供し、当該管理装置から受けたコンテンツファイルを前記データベースに格納し、

前記管理装置は、対応する前記データ提供装置から受けた前記マスソースをコンテンツ鍵データを用いて暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データ提供装置に送り、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを対応する前記データ配給装置に送り、

前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルと、前記管理装置から提供を受けたキーファイルとを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定するデータ提供システム。

【請求項 1 3 8】

複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を有するデータ提供システムにおいて、

前記データ提供装置は、コンテンツデータのマスソースに対応する前記管理装置に提供し、当該管理装置から受けたコンテンツファイルを前記データベースに格納し、

前記管理装置は、対応する前記データ提供装置から受けた前記マスソースをコンテンツ鍵データを用いて暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データ提供装置に送り、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に提供し、

前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定するデータ提供システム。

【請求項 1 3 9】

データ提供装置、データ配給装置およびデータ処理装置を有するデータ提供システムにおいて、

前記データ提供装置は、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納した第1のモジュールを前記データ配給装置に提供し、前記データ処理装置から受けた履歴データに基づいて、コンテンツデータ単位で課金処理を行い、前記データ処理装置の関係者が支払った利益を当該データ提供装置の関係者と前記データ配給装置の関係者とに分配する利益分配処理を行い、

前記データ配給装置は、前記提供を受けた前記第1のモジュールに格納された前記暗号化されたコンテンツデータ、コンテンツ鍵データおよび権利書データを格納した第2のモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定し、当該コンテンツデータの取り扱いについての履歴データを作成し、当該履歴データを前記データ提供装置に送る

データ提供システム。

【請求項140】

前記データ処理装置は、前記データ配給装置が行うコンテンツデータの配信サービスに関してのデータ配給装置用履歴データを前記データ配給装置に送り、

前記データ配給装置は、前記データ配給装置用履歴データに基づいて、課金処理を行う

請求項139に記載のデータ提供システム。

【請求項141】

データ提供装置、データ配給装置、データ処理装置および管理装置を有するデータ提供システムにおいて、

前記データ提供装置は、コンテンツデータを提供し、

前記データ配給装置は、前記データ提供装置から提供を受けた前記コンテンツ

ファイル、あるいは前記管理装置から提供を受けた前記データ提供装置が提供したコンテンツデータに応じたコンテンツファイルを前記データ処理装置に配給し

、
前記データ処理装置は、前記データ配給装置あるいは前記管理装置から受けたキーファイルに格納された権利書データを復号し、当該復号した権利書データに基づいて、前記データ配給装置あるいは前記管理装置から受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定し、前記データ配給装置あるいは前記管理装置から受けた前記コンテンツファイルおよびキーファイルをさらに他のデータ処理装置に配信する

データ提供システム。

【請求項 142】

データ提供装置からデータ処理装置にコンテンツデータを配給するデータ提供方法において、

コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ提供装置から前記データ処理装置に配給し、

前記データ処理装置において、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する

データ提供方法。

【請求項 143】

データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法において、

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、

前記作成したキーファイルを前記管理装置から前記データ提供装置に配給し、
前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から配給を受けた前記キーファイルとを格納したモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ提供装置から前記データ処理装置に配給し、

前記データ処理装置において、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する

データ提供方法。

【請求項 144】

データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法において、

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、

前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けたキーファイルとを含むコンテンツファイルを格納したモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置において、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する

データ提供方法。

【請求項 145】

データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法

において、

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、

当該作成したキーファイルを前記管理装置から前記データ提供装置に配給し、

前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して個別に前記データ提供装置から前記データ処理装置に配給し、

前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供方法。

【請求項 1 4 6】

データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法において、

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、

当該作成したキーファイルを前記管理装置から前記データ処理装置に配給し、

前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ提供装置から前記データ処理装置に配給し、

前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツファイルに格納されたコ

ンテンツデータの取り扱いを決定する

データ提供方法。

【請求項 147】

データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法において、

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、

前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記キーファイルとを格納したモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置において、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する

データ提供方法。

【請求項 148】

データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法において、

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、

前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記キーファイルとを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して個別に前記データ処理装置に配給し、

前記データ処理装置において、前記配給を受けた前記キーファイルに格納され

た前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツデータの取り扱いを決定するデータ提供方法。

【請求項 1 4 9】

データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法において、

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に配給し、

前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツデータの取り扱いを決定する

データ提供方法。

【請求項 1 5 0】

データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法において、

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを作成し、

前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記暗号化されたコンテンツ鍵データおよび前記暗号化された権利書データとを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して個別に前記データ処理装置に配給し、

前記データ処理装置において、前記配給を受けた前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供方法。

【請求項 151】

データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法において、

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを作成して前記データ処理装置に配給し、

前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置において、前記配給を受けた前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツデータの取り扱いを決定する

データ提供方法。

【請求項 152】

データ提供装置、データ配給装置およびデータ処理装置を用いたデータ提供方法において、

コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納した第1のモジュールを前記データ提供装置から前記データ配給装置に提供し、

前記提供を受けた前記第1のモジュールに格納された前記暗号化されたコンテンツデータ、コンテンツ鍵データおよび権利書データを格納した第2のモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、

あるいは記録媒体に記録して前記データ配給装置から前記データ処理装置に配給し、

前記データ処理装置において、前記配給を受けた前記第2のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する

データ提供方法。

【請求項153】

データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供方法において、

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、

当該作成したキーファイルを前記管理装置から前記データ提供装置に配給し、

前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとを格納した第1のモジュールを、前記データ提供装置から前記データ配給装置に提供し、

前記提供を受けたコンテンツファイルおよび前記キーファイルを格納した第2のモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ配給装置から前記データ処理装置に配給し、

前記データ処理装置において、前記配給を受けた前記第2のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記第2のモジュールに格納された前記コンテンツデータの取り扱いを決定する

データ提供方法。

【請求項154】

データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ

配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供方法において、

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、

前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと前記管理装置から受けたキーファイルとを含むコンテンツファイルを格納した第 1 のモジュールを前記データ配給装置に提供し、

前記データ配給装置において、前記提供を受けたコンテンツファイルを格納した第 2 のモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置において、前記配給を受けた前記第 2 のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記第 2 のモジュールに格納された前記コンテンツデータの取り扱いを決定する

データ提供方法。

【請求項 1 5 5】

データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供方法において、

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、

前記作成したキーファイルを前記管理装置から前記データ提供装置に配給し、

前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒

体に記録して個別に前記データ提供装置から前記データ配給装置に配給し、

前記配給を受けた前記コンテンツファイルと前記キーファイルとを個別に前記データ配給装置から前記データ配給装置に配給し、

前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供方法。

【請求項 1 5 6】

データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法において、

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、

当該作成したキーファイルを前記管理装置から前記データ処理装置に配給し、

前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルを前記データ提供装置から前記データ配給装置に提供し、

前記提供を受けたコンテンツファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ配給装置から前記データ処理装置に配給し、

前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供方法。

【請求項 1 5 7】

データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前

記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供方法において、

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、

前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記キーファイルとを格納した第 1 のモジュールを前記データ配給装置に提供し、

前記データ配給装置において、前記提供を受けたコンテンツデータおよび前記キーファイルを格納した第 2 のモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置において、前記配給を受けた前記第 2 のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記第 2 のモジュールに格納された前記コンテンツデータの取り扱いを決定する

データ提供方法。

【請求項 1 5 8】

データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供方法において、

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、

前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記キーファイルとを個別に前記データ配給装置に配給し、

前記データ配給装置において、配給を受けた前記コンテンツデータと前記キー

ファイルとを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して個別に前記データ配給装置に配給し、

前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツデータの取り扱いを決定するデータ提供方法。

【請求項 159】

データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法において、

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に配給し、

前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを前記データ配給装置に提供し、

前記データ配給装置において、前記提供を受けたコンテンツデータを前記データ処理装置に配給し、

前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツデータの取り扱いを決定する

データ提供方法。

【請求項 160】

データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供方法において、

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを前記データ提供装置に提供

し、

前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記暗号化されたコンテンツ鍵データおよび前記暗号化された権利書データとを個別に前記データ配給装置に配給し、

前記データ配給装置において、配給を受けた前記コンテンツデータと前記暗号化されたコンテンツ鍵データおよび前記暗号化された権利書データとを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して個別に前記データ配給装置に配給し、

前記データ処理装置において、前記配給を受けた前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツデータの取り扱いを決定する

データ提供方法。

【請求項 161】

データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供方法において、

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを前記データ処理装置に配給し、

前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを前記データ配給装置に提供し、

前記データ配給装置は、前記提供を受けたコンテンツデータを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置において、前記配給を受けた前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツデータの取り扱いを決定する

データ提供方法。

【請求項 162】

データ提供装置、データ配給装置、管理装置およびデータ処理装置を用いたデータ提供方法において、

前記データ提供装置は、コンテンツのマスターソースデータを前記管理装置に提供し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置を管理し、前記提供されたマスターソースデータをコンテンツ鍵データを用いて暗号化してコンテンツデータを作成し、当該コンテンツデータを格納したコンテンツファイルを作成し、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記コンテンツファイルおよび前記キーファイルを前記データ配給装置に提供し、

前記データ配給装置は、前記提供を受けた前記コンテンツファイルおよび前記キーファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供方法。

【請求項 163】

データ提供装置、データ配給装置、管理装置およびデータ処理装置を用いたデータ提供方法において、

前記データ提供装置は、コンテンツのマスターソースデータを前記管理装置に提供し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置を管理し、前記提供されたマスターソースデータをコンテンツ鍵データを用いて暗号化してコンテンツデータを作成し、当該コンテンツデータを格納した

コンテンツファイルを作成し、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記コンテンツファイルを前記データ配給装置に提供し、前記キーファイルを前記データ処理装置に提供し、

前記データ配給装置は、前記提供を受けた前記コンテンツファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供方法。

【請求項 164】

データ提供装置、データ配給装置、管理装置およびデータ処理装置を用いたデータ提供方法において、

前記データ提供装置は、コンテンツ鍵データを用いた暗号化したコンテンツデータを格納したコンテンツファイルを前記管理装置に提供し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置を管理し、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置から提供を受けた前記コンテンツファイルと、前記作成したキーファイルとを前記データ配給装置に提供し、

前記データ配給装置は、前記提供を受けた前記コンテンツファイルおよび前記キーファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供方法。

【請求項 1 6 5】

データ提供装置、データ配給装置、管理装置およびデータ処理装置を用いたデータ提供方法において、

前記データ提供装置は、コンテンツ鍵データを用いた暗号化したコンテンツデータを格納したコンテンツファイルを前記管理装置に提供し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置を管理し、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置から提供を受けた前記コンテンツファイルを前記データ配給装置に提供し、前記作成したキーファイルを前記データ処理装置に提供し、

前記データ配給装置は、前記提供を受けた前記コンテンツファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供方法。

【請求項 1 6 6】

データ提供装置、データ配給装置、管理装置、データベース装置およびデータ処理装置を用いたデータ提供方法において、

前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルおよび前記管理装置から提供を受けたキーファイルを前記データベース装置に格納し、

前記管理装置は、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作

成し、当該作成したキーファイルを前記データ提供装置に提供し、

前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルおよびキーファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供方法。

【請求項 167】

データ提供装置、データ配給装置、管理装置、データベース装置およびデータ処理装置を用いたデータ提供方法において、

前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データベース装置に格納し、

前記管理装置は、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ配給装置に提供し、

前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルと、前記データ配給装置から提供を受けたキーファイルとを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供方法。

【請求項 168】

データ提供装置、データ配給装置、管理装置、データベース装置およびデータ

処理装置を用いたデータ提供方法において、

前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データベース装置に格納し、

前記管理装置は、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に提供し、

前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供方法。

【請求項 1 6 9】

複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を用いたデータ提供方法において、

前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルおよび対応する前記管理装置から提供を受けたキーファイルを前記データベース装置に格納し、

前記管理装置は、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを対応する前記データ提供装置に提供し、

前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルおよびキーファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供方法。

【請求項 170】

複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を用いたデータ提供方法において、

前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データベース装置に格納し、

前記管理装置は、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ配給装置に提供し、

前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルと、前記管理装置から提供を受けたキーファイルとを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供方法。

【請求項 171】

複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を用いたデータ提供方法において、

前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し

、当該作成したコンテンツファイルを前記データベース装置に格納し、

前記管理装置は、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に提供し、

前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供方法。

【請求項 172】

複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を用いたデータ提供方法において、

前記データ提供装置は、コンテンツデータのマスソースを対応する前記管理装置に提供し、当該管理装置から受けたコンテンツファイルおよびキーファイルを前記データベースに格納し、

前記管理装置は、対応する前記データ提供装置から受けた前記マスソースをコンテンツ鍵データを用いて暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記作成したコンテンツファイルおよび前記作成したキーファイルを対応する前記データ提供装置に送り、

前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルおよびキーファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供方法。

【請求項 173】

複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を用いたデータ提供方法において、

前記データ提供装置は、コンテンツデータのマスソースを対応する前記管理装置に提供し、当該管理装置から受けたコンテンツファイルを前記データベースに格納し、

前記管理装置は、対応する前記データ提供装置から受けた前記マスソースをコンテンツ鍵データを用いて暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データ提供装置に送り、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを対応する前記データ配給装置に送り、

前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルと、前記管理装置から提供を受けたキーファイルとを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供方法。

【請求項 174】

複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置

およびデータ処理装置を用いたデータ提供方法において、

前記データ提供装置は、コンテンツデータのマスソースを対応する前記管理装置に提供し、当該管理装置から受けたコンテンツファイルを前記データベースに格納し、

前記管理装置は、対応する前記データ提供装置から受けた前記マスソースをコンテンツ鍵データを用いて暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データ提供装置に送り、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に提供し、

前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

データ提供方法。

【請求項 175】

データ提供装置、データ配給装置およびデータ処理装置を用いたデータ提供方法において、

前記データ提供装置は、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納した第1のモジュールを前記データ配給装置に提供し、前記データ処理装置から受けた履歴データに基づいて、コンテンツデータ単位で課金処理を行い、前記データ処理装置の関係者が支払った利益を当該データ提供装置の関係者と前記データ配給装置の関係者とに分配する利益分配処理を行い、

前記データ配給装置は、前記提供を受けた前記第1のモジュールに格納された前記暗号化されたコンテンツデータ、コンテンツ鍵データおよび権利書データを格納した第2のモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定し、当該コンテンツデータの取り扱いについての履歴データを作成し、当該履歴データを前記データ提供装置に送る

データ提供方法。

【請求項 176】

データ提供装置、データ配給装置、データ処理装置および管理装置を用いたデータ提供方法において、

前記データ提供装置は、コンテンツデータを提供し、

前記データ配給装置は、前記データ提供装置から提供を受けた前記コンテンツファイル、あるいは前記管理装置から提供を受けた前記データ提供装置が提供したコンテンツデータに応じたコンテンツファイルを前記データ処理装置に配給し、

前記データ処理装置は、前記データ配給装置あるいは前記管理装置から受けたキーファイルに格納された権利書データを復号し、当該復号した権利書データに基づいて、前記データ配給装置あるいは前記管理装置から受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定し、前記データ配給装置あるいは前記管理装置から受けた前記コンテンツファイルおよびキーファイルをさらに他のデータ処理装置に配信する

データ提供方法。

【請求項 177】

データ提供装置からデータ処理装置にコンテンツデータを配給するデータ提供システムにおいて、

前記データ提供装置は、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを前記コンテンツデータの圧縮の有無、圧縮方式、前記暗号化の方式およびコンテンツデータを得た信号の諸元の少なくとも一つに依存しない形式で格納したモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する

データ提供システム。

【請求項 178】

前記データ提供装置は、自らの署名データを当該署名データの作成方式に依存しない形式でさらに格納した前記モジュールを前記データ処理装置に配給する
請求項 177 に記載のデータ提供システム。

【請求項 179】

データ提供装置、データ配給装置およびデータ処理装置を有するデータ提供システムにおいて、

前記データ提供装置は、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを前記コンテンツデータの圧縮の有無、圧縮方式、前記暗号化の方式およびコンテンツデータを得た信号の諸元の少なくとも一つに依存しない形式で格納した第 1 のモジュールを前記データ配給装置に提供し、

前記データ配給装置は、前記提供を受けた前記第 1 のモジュールに格納された前記暗号化されたコンテンツデータ、コンテンツ鍵データおよび権利書データを格納した第 2 のモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記第2のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する

データ提供システム。

【請求項180】

前記データ提供装置は、自らの署名データを当該署名データの作成方式に依存しない形式でさらに格納した前記第1のモジュールを前記データ配給装置に提供する

請求項179に記載のデータ提供システム。

【請求項181】

データ提供装置、データ配給装置およびデータ処理装置を有するデータ提供システムにおいて、

前記データ提供装置は、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納した第1のモジュールを前記データ配給装置に提供し、

前記データ配給装置は、前記提供を受けた前記第1のモジュールに格納された前記暗号化されたコンテンツデータ、コンテンツ鍵データおよび権利書データを格納した複数の第2のモジュールを、前記データ処理装置との間の相互認証によって得られた共有鍵を用いて暗号化した後に、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記複数の第2のモジュールを前記共有鍵を用いて復号し、当該復号した前記複数の第2のモジュールのなかから単数または複数の第2のモジュールを選択し、前記第2のモジュールの配給サービスに対しての課金処理を行う第1の処理回路と、前記選択された前記第2のモジュールを受けて当該第2のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する耐タンパ性の第2の処理回路とを有する

データ提供システム。

【請求項 1 8 2】

前記第 1 の処理回路は、前記データ配給装置の前記第 2 のモジュールの配給サービスに関してのデータ配給装置用履歴データを作成し、当該データ配給装置用履歴データを前記データ配給装置に送り、

前記データ配給装置は、前記データ配給装置用履歴データに基づいて課金処理を行う

請求項 1 8 1 に記載のデータ提供システム。

【請求項 1 8 3】

前記データ提供装置、前記データ配給装置および前記データ処理装置を管理する管理装置をさらに有し、

前記第 2 の処理回路は、前記コンテンツデータの取り扱いを決定し、当該決定に応じた利用履歴データを作成し、当該利用履歴データを前記管理装置に送り、

前記管理装置は、前記利用履歴データに基づいて、前記データ処理装置の関係者が支払った前記コンテンツデータに関しての利益を前記データ提供装置および前記データ配給装置の関係者に分配する利益分配処理を行う

請求項 1 8 1 に記載のデータ提供システム。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、コンテンツデータを提供するデータ提供システムおよびその方法、データ提供装置およびデータ処理装置に関する。

【0 0 0 2】

【従来の技術】

暗号化されたコンテンツデータを所定の契約を交わしたユーザのデータ処理装置に配給し、当該データ処理装置において、コンテンツデータを復号して再生および記録するデータ提供システムがある。

このようなデータ提供システムの一つに、音楽データを配信する従来の EMD (Electronic Music Distribution: 電子音楽配信) システムがある。

【0003】

図145は、従来のEMDシステム700の構成図である。

図145に示すEMDシステム700では、コンテンツプロバイダ701a, 701bが、サービスプロバイダ710に対し、コンテンツデータ704a, 704b, 704cと、著作権情報705a, 705b, 705cとを、それぞれ相互認証後に得たセッション鍵データで暗号化してオンラインで供給したり、あるいはオフラインで供給する。ここで、著作権情報705a, 705b, 705cには、例えば、SCMS (Serial Copy Management System) 情報、コンテンツデータに埋め込むことを要請する電子透かし情報およびサービスプロバイダ710の伝送プロトコルに埋め込むことを要請する著作権に関する情報などがある。

【0004】

サービスプロバイダ710は、受信したコンテンツデータ704a, 704b, 704cと、著作権情報705a, 705b, 705cとをセッション鍵データを用いて復号する。

そして、サービスプロバイダ710は、復号したあるいはオフラインで受け取ったコンテンツデータ704a, 704b, 704cに、著作権情報705a, 705b, 705cを埋め込んで、コンテンツデータ707a, 707b, 707cを生成する。このとき、サービスプロバイダ710は、例えば、著作権情報705a, 705b, 705cのうち電子透かし情報をコンテンツデータ704a, 704b, 704cに所定の周波数領域を変更して埋め込み、当該コンテンツデータをユーザに送信する際に用いるネットワークプロトコルにSCMS情報を埋め込む。

さらに、サービスプロバイダ710は、コンテンツデータ707a, 707b, 707cを、鍵データベース706から読み出したコンテンツ鍵データKca, Kcb, Kccを用いてそれぞれ暗号化する。その後、サービスプロバイダ710は、暗号化されたコンテンツデータ707a, 707b, 707cを格納したセキュアコンテナ722を、相互認証後に得たセッション鍵データによって暗号化してユーザの端末装置709に存在するCA (Conditional A

c c e s s) モジュール 711 に送信する。

【0005】

CAモジュール 711 は、セキュアコンテナ 722 をセッション鍵データを用いて復号する。また、CAモジュール 711 は、電子決済やCAなどの課金機能を用いて、サービスプロバイダ 710 の鍵データベース 706 からコンテンツ鍵データ K c a, K c b, K c c を受信し、これをセッション鍵データを用いて復号する。これにより、端末装置 709 において、コンテンツデータ 707 a, 707 b, 707 c を、それぞれコンテンツ鍵データ K c a, K c b, K c c を用いて復号することが可能になる。

このとき、CAモジュール 711 は、コンテンツ単位で課金処理を行い、その結果に応じた課金情報 721 を生成し、これをセッション鍵データで暗号化した後に、サービスプロバイダ 710 の権利処理モジュール 720 に送信する。

この場合に、CAモジュール 711 は、サービスプロバイダ 710 が自らの提供するサービスに関して管理したい項目であるユーザの契約（更新）情報および月々基本料金などのネットワーク家賃の徴収と、コンテンツ単位の課金処理と、ネットワークの物理層のセキュリティ確保とを行う。

【0006】

サービスプロバイダ 710 は、CAモジュール 711 から課金情報 721 を受信すると、サービスプロバイダ 710 とコンテンツプロバイダ 701 a, 701 b, 701 c との間で利益配分を行う。

このとき、サービスプロバイダ 710 から、コンテンツプロバイダ 701 a, 701 b, 701 c への利益配分は、例えば、JASRAC (Japanese Society for Rights of Authors, Composers and Publishers: 日本音楽著作権協会) を介して行われる。また、JASRAC によって、コンテンツプロバイダの利益が、当該コンテンツデータの著作権者、アーティスト、作詞・作曲家および所属プロダクションなどに分配される。

【0007】

また、端末装置 709 では、コンテンツ鍵データ K c a, K c b, K c c を用

いて復号したコンテンツデータ 707a, 707b, 707c を、RAM 型の記録媒体 723 などに記録する際に、著作権情報 705a, 705b, 705c の SCMS ビットを書き換えて、コピー制御を行う。すなわち、ユーザ側では、コンテンツデータ 707a, 707b, 707c に埋め込まれた SCMS ビットに基づいて、コピー制御が行われ、著作権の保護が図られている。

【0008】

【発明が解決しようとする課題】

ところで、SCMS は、コンテンツデータを例えば 2 世代以上のわたって複製することを禁止するものであり、1 世代の複製は無制限に行うことができ、著作権者の保護として不十分であるという問題がある。

【0009】

また、上述した EMD システム 700 では、サービスプロバイダ 710 が暗号化されていないコンテンツデータを技術的に自由に扱えるため、コンテンツプロバイダ 701 の関係者はサービスプロバイダ 710 の行為等を監視する必要があり、当該監視の負担が大きいと共に、コンテンツプロバイダ 701 の利益が不当に損なわれる可能性が高いという問題がある。

また、上述した EMD システム 700 では、ユーザの端末装置 709 がサービスプロバイダ 710 から配給を受けたコンテンツデータをオーサリングして他の端末装置などに再配給する行為を規制することが困難であり、コンテンツプロバイダ 701 の利益が不当に損なわれるという問題がある。

【0010】

本発明は上述した従来技術の問題点に鑑みてなされ、コンテンツプロバイダの権利者（関係者）の利益を適切に保護できるデータ提供システムおよびその方法、データ提供装置およびデータ処理装置を提供することを目的とする。

また、本発明は、コンテンツプロバイダの権利者の利益を保護するための監査の負担を軽減できるデータ提供システムおよびその方法、データ提供装置およびデータ処理装置を提供することを目的とする。

【0011】

【課題を解決するための手段】

上述した従来技術の問題点を解決し、上述した目的を達成するために、本発明の第 1 の観点のデータ提供システムは、データ提供装置からデータ処理装置にコンテンツデータを配給するデータ提供であって、前記データ提供装置は、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する。

【 0 0 1 2 】

本発明の第 1 の観点のデータ提供システムの作用は以下に示すようになる。

前記データ提供装置から前記データ処理装置に、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したモジュールが配給される。

このとき、当該モジュールは、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式、あるいは記録媒体に記録されて前記データ提供装置から前記データ処理装置に配給される。

そして、前記データ処理装置において、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いが決定される。

このように、コンテンツデータを格納したモジュールに、当該コンテンツデータの取り扱いを示す権利書データを格納することで、データ処理装置において、データ提供装置の関係者が作成した権利書データに基づいたコンテンツデータの取り扱い（利用）を行わせることが可能になる。

また、前記モジュールは、所定の通信プロトコルに依存しない形式で前記データ提供装置から前記データ処理装置に配給されることから、前記モジュールに格納されるコンテンツデータの圧縮方式や暗号化方式などを前記データ提供装置が

任意に決定できる。

【0013】

また、本発明の第1の観点のデータ提供システムは、好ましくは、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データのうち少なくとも一つのデータの作成者および送信者の正当性を検証するための署名データをさらに格納した前記モジュールを前記データ処理装置に配給する。

【0014】

また、本発明の第1の観点のデータ提供システムは、好ましくは、前記データ提供装置は、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データのうち少なくとも一つのデータについて、当該データが改竄されていないかを検証するためのデータと、当該データを所定の機関によって正規に認証されているかを検証するための署名データとのうち少なくとも一方のデータをさらに格納した前記モジュールを前記データ処理装置に配給する。

【0015】

また、本発明の第1の観点のデータ提供システムは、好ましくは、前記データ処理装置は、前記権利書データに基づいて、前記コンテンツデータの購入形態を決定し、前記コンテンツデータを他のデータ処理装置に転送する場合に、当該コンテンツデータの購入者の正当性を示す署名データと、当該コンテンツデータの送信者の正当性を示す署名データとを異ならせる。

【0016】

本発明の第2の観点のデータ提供システムは、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとを格納したモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ

処理装置は、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する。

【0017】

本発明の第2の観点のデータ提供システムの作用は以下に示すようになる。

管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルが作成される。

そして、当該作成されたキーファイルが、前記管理装置から前記データ提供装置に配給される。

そして、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとを格納したモジュールが、前記データ提供装置から前記データ処理装置に所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して配給される。

そして、前記データ処理装置において、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データが復号され、当該復号された権利書データに基づいて、前記コンテンツデータの取り扱いが決定される。

。

【0018】

また、本発明の第2の観点のデータ提供システムは、好ましくは、前記管理装置は、前記キーファイルの作成者の正当性を検証するための署名データを生成し、当該署名データをさらに格納した前記キーファイルを作成する。

【0019】

また、本発明の第2の観点のデータ提供システムは、好ましくは、前記データ提供装置は、前記コンテンツ鍵データおよび前記権利書データを生成して前記管理装置に送信し、前記管理装置は、受信した前記コンテンツ鍵データおよび前記権利書データに基づいて前記キーファイルを作成し、当該作成したキーファイルを登録する。

【 0 0 2 0 】

また、本発明のデータ提供装置は、管理装置によって管理され、データ処理装置にコンテンツデータを配給するデータ提供装置であって、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを前記管理装置から受け、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとを格納したモジュールを前記データ処理装置に配給する。

【 0 0 2 1 】

また、本発明のデータ処理装置は、管理装置によって管理され、コンテンツデータを利用するデータ処理装置であって、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルと、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルとを含むモジュールを受け、前記権利書データに基づいて、前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の少なくとも一方の履歴を示す履歴データを前記管理装置に送信する。

【 0 0 2 2 】

また、本発明の第 3 の観点のデータ提供システムは、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けたキーファイルとを含むコンテンツファイルを格納したモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前

記コンテンツデータの取り扱いを決定する。

【0023】

本発明の第3の観点のデータ提供システムの作用は以下に示すようになる。

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルが作成され、当該キーファイルが前記データ提供装置に送られる。

そして、前記データ提供装置から前記データ処理装置に、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けたキーファイルとを含むコンテンツファイルを格納したモジュールが、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して配給される。

そして、前記データ処理装置において、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データが復号され、当該復号され権利書データに基づいて、前記コンテンツデータの取り扱いが決定される。

【0024】

本発明の第4の観点のデータ提供システムは、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して個別に前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する

【0025】

本発明の第4の観点のデータ提供システムの作用は以下に示すようになる。

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルが作成され、当該キーファイルが前記データ提供装置に送られる。

そして、前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとが、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して個別に前記データ処理装置に配給される。

そして、前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データが復号され、当該復号された権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いが決定される。

【0026】

また、本発明の第5の観点のデータ提供システムは、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に配給し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

【0027】

以下、本発明の第5の観点のデータ提供システムの作用を説明する。

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデ

ータの取り扱いを示す暗号化された権利書データとを格納したキーファイルが作成される。

当該作成されたキーファイルは、前記管理装置から前記データ処理装置に配給される。

また、前記データ提供装置から前記データ処理装置に、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルが、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して配給される。

そして、前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データが復号され、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツファイルに格納されたコンテンツデータの取り扱いが決定される。

【 0 0 2 8 】

また、本発明の第 6 の観点のデータ提供システムは、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記キーファイルとを格納したモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する。

【 0 0 2 9 】

以下、本発明の第 6 の観点のデータ提供システムの作用を説明する。

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルが作

成され、当該キーファイルが前記データ提供装置に送られる。

そして、前記データ提供装置から前記データ処理装置に、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記キーファイルとを格納したモジュールが、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して配給される。

そして、前記データ処理装置において、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データが復号し、当該復号された権利書データに基づいて、前記コンテンツデータの取り扱いが決定される。

【0030】

また、本発明の第7の観点のデータ提供システムは、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記キーファイルとを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して個別に前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツデータの取り扱いを決定する。

【0031】

以下、本発明の第7の観点のデータ提供システムの作用を説明する。

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルが作成され、当該キーファイルが前記データ提供装置に送られる。

そして、前記データ提供装置から前記データ処理装置に、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記キ

ーファイルとが、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して個別に配給される。

そして、前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データが復号され、当該復号された権利書データに基づいて、前記配給を受けたコンテンツデータの取り扱いが決定される。

【0032】

また、本発明の第8の観点のデータ提供システムは、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に配給し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツデータの取り扱いを決定する。

【0033】

以下、本発明の第8の観点のデータ提供システムの作用を説明する。 前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルが作成され、当該作成されたキーファイルが前記データ処理装置に配給される。

また、前記データ提供装置から前記データ処理装置に、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータが、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して配給される。

そして、前記データ処理装置において、前記配給を受けた前記キーファイルに

格納された前記コンテンツ鍵データおよび前記権利書データが復号され、当該復号された権利書データに基づいて、前記配給を受けた前記コンテンツデータの取り扱いが決定される。

【 0 0 3 4 】

また、本発明の第 9 の観点のデータ提供システムは、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを作成し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記暗号化されたコンテンツ鍵データおよび前記暗号化された権利書データとを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して個別に前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

【 0 0 3 5 】

以下、本発明の第 9 の観点のデータ提供システムの作用を説明する。

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとが作成され、これらが前記データ提供装置に送られる。

そして、前記データ提供装置から前記データ処理装置に、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記暗号化されたコンテンツ鍵データおよび前記暗号化された権利書データとが、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して個別に配給される。

そして、前記データ処理装置において、前記配給を受けた前記コンテンツ鍵データおよび前記権利書データが復号され、当該復号された権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り

扱いが決定される。

データ提供システム。

【0036】

また、本発明の第10の観点のデータ提供システムは、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを作成して前記データ処理装置に配給し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツデータの取り扱いを決定する。

【0037】

以下、本発明の第10の観点のデータ提供システムの作用を説明する。

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとが作成され、これらが前記データ処理装置に配給される。

また、前記データ提供装置から前記データ処理装置に、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータが、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して配給される。

そして、前記データ処理装置において、前記配給を受けた前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツデータの取り扱いが決定される。

【0038】

また、本発明の第11の観点のデータ提供システムは、データ提供装置、データ配給装置およびデータ処理装置を有するデータ提供システムであって、前記デ

ータ提供装置は、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納した第1のモジュールを前記データ配給装置に提供し、前記データ配給装置は、前記提供を受けた前記第1のモジュールに格納された前記暗号化されたコンテンツデータ、コンテンツ鍵データおよび権利書データを格納した第2のモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記第2のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する。

【0039】

以下、本発明の第11の観点のデータ提供システムの作用を説明する。

前記データ提供装置から前記データ配給装置に、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納した第1のモジュールが、例えば、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して提供される。

次に、前記データ配給装置から前記データ処理装置に、前記提供を受けた前記第1のモジュールに格納された前記暗号化されたコンテンツデータ、コンテンツ鍵データおよび権利書データを格納した第2のモジュールが、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して配給される。

そして、前記データ処理装置において、前記配給を受けた前記第2のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データが復号され、当該復号された権利書データに基づいて、前記コンテンツデータの取り扱いが決定される。

このように、コンテンツデータを格納した第1のモジュールおよび第2のモジュールに、当該コンテンツデータの取り扱いを示す権利書データを格納すること

で、データ処理装置において、データ提供装置の関係者が作成した権利書データに基づいたコンテンツデータの取り扱い（利用）を行わせることが可能になる。

また、前記第2のモジュールは、所定の通信プロトコルに依存しない形式で前記データ配給装置から前記データ処理装置に配給されることから、前記第2のモジュールに格納されるコンテンツデータの圧縮方式や暗号化方式などを前記データ提供装置が任意に決定できる。

【0040】

本発明の第12の観点のデータ提供システムは、データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとを格納した第1のモジュールを前記データ配給装置に提供し、前記データ配給装置は、前記提供を受けたコンテンツファイルおよび前記キーファイルを格納した第2のモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記第2のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記第2のモジュールに格納された前記コンテンツデータの取り扱いを決定する。

【0041】

以下、本発明の第12の観点のデータ提供システムの作用を説明する。

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルが作成され、当該キーファイルが前記データ提供装置に送られる。

そして、前記データ提供装置から前記データ配給装置に、前記コンテンツ鍵デ

ータを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとを格納した第1のモジュールが提供される。

そして、前記データ配給装置から前記データ処理装置に、前記提供を受けたコンテンツファイルおよび前記キーファイルを格納した第2のモジュールが、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して配給される。

そして、前記データ処理装置において、前記配給を受けた前記第2のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データが復号され、当該復号された権利書データに基づいて、前記配給を受けた前記第2のモジュールに格納された前記コンテンツデータの取り扱いが決定される。

【0042】

また、本発明の第13の観点のデータ提供システムは、データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと前記管理装置から受けたキーファイルとを含むコンテンツファイルを格納した第1のモジュールを前記データ配給装置に提供し、前記データ配給装置は、前記提供を受けたコンテンツファイルを格納した第2のモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記第2のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記第2のモジュールに格納された前記コンテンツデータの取り扱いを決定する。

【0043】

また、本発明の第14の観点のデータ提供システムは、データ提供装置から第1のデータ配給装置および第2のデータ配給装置にコンテンツデータを提供し、前記第1のデータ配給装置および前記第2のデータ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記第1のデータ配給装置、前記第2のデータ配給装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとを格納した第1のモジュールを前記第1のデータ配給装置および前記第2のデータ配給装置に提供し、前記第1のデータ配給装置は、前記提供を受けたコンテンツファイルおよび前記キーファイルを格納した第2のモジュールを前記データ処理装置に配給し、前記第2のデータ配給装置は、前記提供を受けたコンテンツファイルおよび前記キーファイルを格納した第3のモジュールを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記第2のモジュールおよび前記第3のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する。

【0044】

また、本発明の第15の観点のデータ提供システムは、第1のデータ提供装置からデータ配給装置に第1のコンテンツデータを提供し、第2のデータ提供装置からデータ配給装置に第2のコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記第1のデータ提供装置、前記第2のデータ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化された第1のコンテンツ鍵データと前記第1のコンテンツデータの取り扱いを示す暗号化された第1の権利書データとを格納した第1のキーファイルと、暗号化された第2のコンテンツ鍵データと前記第2のコンテンツデータの取り扱いを示す暗号化された第2の権利書データとを格納した第2のキーファイルとを作成し、

前記第1のデータ提供装置は、前記第1のコンテンツ鍵データを用いて暗号化された前記第1のコンテンツデータを格納した第1のコンテンツファイルと、前記管理装置から受けた前記第1のキーファイルとを格納した第1のモジュールを前記データ配給装置に提供し、前記第2のデータ提供装置は、前記第2のコンテンツ鍵データを用いて暗号化された前記第2のコンテンツデータを格納した第2のコンテンツファイルと、前記管理装置から受けた前記第2のキーファイルとを格納した第2のモジュールを前記データ配給装置に提供し、前記データ配給装置は、前記提供を受けた前記第1のコンテンツファイル、前記第1のキーファイル、前記第2のコンテンツファイルおよび前記第2のキーファイルを格納した第3のモジュールを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記第3のモジュールに格納された前記第1のコンテンツ鍵データ、前記第2のコンテンツ鍵データ、前記第1の権利書データおよび前記第2の権利書データを復号し、当該復号した第1の権利書データに基づいて前記第1のコンテンツデータの取り扱いを決定し、前記復号した第2の権利書データに基づいて前記第2のコンテンツデータの取り扱いを決定する。

【0045】

また、本発明の第16の観点のデータ提供システムは、データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとを個別に前記データ配給装置に配給し、前記データ配給装置は、配給を受けた前記コンテンツファイルと前記キーファイルとを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して個別に前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書デ

タを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

【0046】

また、本発明の第17の観点のデータ提供システムは、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に配給し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルを前記データ配給装置に提供し、前記データ配給装置は、前記提供を受けたコンテンツファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

【0047】

また、本発明の第18の観点のデータ提供システムは、データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記キーファイルとを格納した第1のモジュールを前記データ配給装置に提供し、前記データ配給装置は、前記提供を受けたコンテンツデータおよび前記キーファイルを格納した第2のモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるい

は記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記第 2 のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記第 2 のモジュールに格納された前記コンテンツデータの取り扱いを決定する。

【 0 0 4 8 】

また、本発明の第 1 9 の観点のデータ提供システムは、データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記キーファイルとを個別に前記データ配給装置に配給し、前記データ配給装置は、配給を受けた前記コンテンツデータと前記キーファイルとを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して個別に前記データ配給装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツデータの取り扱いを決定する。

【 0 0 4 9 】

また、本発明の第 2 0 の観点のデータ提供システムは、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に配給し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを前記データ配給装置に提供し、前記データ配給装置は、前記提供を受けたコンテンツデータを、所定

の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツデータの取り扱いを決定する。

【0050】

また、本発明の第21の観点のデータ提供システムは、データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを前記データ提供装置に提供し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記暗号化されたコンテンツ鍵データおよび前記暗号化された権利書データとを個別に前記データ配給装置に配給し、前記データ配給装置は、配給を受けた前記コンテンツデータと前記暗号化されたコンテンツ鍵データおよび前記暗号化された権利書データとを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して個別に前記データ配給装置に配給し、前記データ処理装置は、前記配給を受けた前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツデータの取り扱いを決定する。

【0051】

また、本発明の第22の観点のデータ提供システムは、データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを前記データ処理装置に配給し、

前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを前記データ配給装置に提供し、前記データ配給装置は、前記提供を受けたコンテンツデータを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツデータの取り扱いを決定する。

【 0 0 5 2 】

また、本発明の第 2 3 の観点のデータ提供システムは、データ提供装置、データ配給装置、管理装置およびデータ処理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツのマスタソースデータを前記管理装置に提供し、前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置を管理し、前記提供されたマスタソースデータをコンテンツ鍵データを用いて暗号化してコンテンツデータを作成し、当該コンテンツデータを格納したコンテンツファイルを作成し、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記コンテンツファイルおよび前記キーファイルを前記データ配給装置に提供し、前記データ配給装置は、前記提供を受けた前記コンテンツファイルおよび前記キーファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

【 0 0 5 3 】

また、本発明の第 2 3 の観点のデータ提供システムは、好ましくは、前記管理装置は、前記コンテンツファイルおよび前記キーファイルを格納した第 1 のモジュールを作成し、当該第 1 のモジュールを前記データ配給装置に提供し、前記データ配給装置は、前記第 1 のモジュールに格納された前記コンテンツファイルお

よび前記キーファイルを格納した第2のモジュールを生成し、当該第2のモジュールを前記データ処理装置に配給する。

【0054】

また、本発明の第23の観点のデータ提供システムは、好ましくは、前記管理装置は、前記コンテンツファイルを記憶および管理するデータベース、前記キーファイルを記憶および管理するデータベース、および前記権利書データを記憶および管理するデータベースのうち、少なくとも一つのデータベースを有し、前記コンテンツデータに固有に割り当てられたコンテンツ識別子を用いて、前記コンテンツファイル、前記キーファイルおよび前記権利書データの少なくとも一つを一元的に管理する。

【0055】

また、本発明の第24の観点のデータ提供システムは、データ提供装置、データ配給装置、管理装置およびデータ処理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツのマスタソースデータを前記管理装置に提供し、前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置を管理し、前記提供されたマスタソースデータをコンテンツ鍵データを用いて暗号化してコンテンツデータを作成し、当該コンテンツデータを格納したコンテンツファイルを作成し、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記コンテンツファイルを前記データ配給装置に提供し、前記キーファイルを前記データ処理装置に提供し、前記データ配給装置は、前記提供を受けた前記コンテンツファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

【0056】

また、本発明の第25の観点のデータ提供システムは、データ提供装置、デー

タ配給装置、管理装置およびデータ処理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツ鍵データを用いた暗号化したコンテンツデータを格納したコンテンツファイルを前記管理装置に提供し、前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置を管理し、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置から提供を受けた前記コンテンツファイルと、前記作成したキーファイルとを前記データ配給装置に提供し、前記データ配給装置は、前記提供を受けた前記コンテンツファイルおよび前記キーファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

【 0 0 5 7 】

また、本発明の第 2 6 の観点のデータ提供システムは、データ提供装置、データ配給装置、管理装置およびデータ処理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツ鍵データを用いた暗号化したコンテンツデータを格納したコンテンツファイルを前記管理装置に提供し、前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置を管理し、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置から提供を受けた前記コンテンツファイルを前記データ配給装置に提供し、前記作成したキーファイルを前記データ処理装置に提供し、前記データ配給装置は、前記提供を受けた前記コンテンツファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイル

に格納されたコンテンツデータの取り扱いを決定する。

【0058】

また、本発明の第27の観点のデータ提供システムは、データ提供装置、データ配給装置、管理装置、データベース装置およびデータ処理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルおよび前記管理装置から提供を受けたキーファイルを前記データベース装置に格納し、前記管理装置は、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ提供装置に提供し、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルおよびキーファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

【0059】

また、本発明の第28の観点のデータ提供システムは、データ提供装置、データ配給装置、管理装置、データベース装置およびデータ処理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データベース装置に格納し、前記管理装置は、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ配給装置に提供し、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルと、前記データ配給装置から提供を受けたキーファイルとを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録し

て前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

【0060】

また、本発明の第29の観点のデータ提供システムは、データ提供装置、データ配給装置、管理装置、データベース装置およびデータ処理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データベース装置に格納し、前記管理装置は、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に提供し、

前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

【0061】

また、本発明の第30の観点のデータ提供システムは、複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルおよび対応する前記管理装置から提供を受けたキーファイルを前記データベース装置に格納し、前記管理装置は、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの

取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを対応する前記データ提供装置に提供し、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルおよびキーファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

【0062】

また、本発明の第31の観点のデータ提供システムは、複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データベース装置に格納し、前記管理装置は、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ配給装置に提供し、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルと、前記管理装置から提供を受けたキーファイルとを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

【0063】

また、本発明の第32の観点のデータ提供システムは、複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を

有するデータ提供システムであって、前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データベース装置に格納し、前記管理装置は、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に提供し、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

【0064】

また、本発明の第33の観点のデータ提供システムは、複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツデータのマスソースを対応する前記管理装置に提供し、当該管理装置から受けたコンテンツファイルおよびキーファイルを前記データベースに格納し、前記管理装置は、対応する前記データ提供装置から受けた前記マスソースをコンテンツ鍵データを用いて暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記作成したコンテンツファイルおよび前記作成したキーファイルを対応する前記データ提供装置に送り、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルおよびキーファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ

処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

【0065】

また、本発明の第34の観点のデータ提供システムは、複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツデータのマスターソースに対応する前記管理装置に提供し、当該管理装置から受けたコンテンツファイルを前記データベースに格納し、前記管理装置は、対応する前記データ提供装置から受けた前記マスターソースをコンテンツ鍵データを用いて暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データ提供装置に送り、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルに対応する前記データ配給装置に送り、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルと、前記管理装置から提供を受けたキーファイルとを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

【0066】

また、本発明の第35の観点のデータ提供システムは、複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツデータのマスターソースに対応する前記管理装置に提供し、当該管理装置から受けたコン

テンツファイルを前記データベースに格納し、前記管理装置は、対応する前記データ提供装置から受けた前記マスタソースをコンテンツ鍵データを用いて暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データ提供装置に送り、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に提供し、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、

前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

【0067】

また、本発明の第36の観点のデータ提供システムは、データ提供装置、データ配給装置およびデータ処理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納した第1のモジュールを前記データ配給装置に提供し、前記データ処理装置から受けた履歴データに基づいて、コンテンツデータ単位で課金処理を行い、前記データ処理装置の関係者が支払った利益を当該データ提供装置の関係者と前記データ配給装置の関係者とに分配する利益分配処理を行い、前記データ配給装置は、前記提供を受けた前記第1のモジュールに格納された前記暗号化されたコンテンツデータ、コンテンツ鍵データおよび権利書データを格納した第2のモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号し

た権利書データに基づいて、前記コンテンツデータの取り扱いを決定し、当該コンテンツデータの取り扱いについての履歴データを作成し、当該履歴データを前記データ提供装置に送る。

【0068】

また、本発明の第37の観点のデータ提供システムは、データ提供装置、データ配給装置、データ処理装置および管理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツデータを提供し、前記データ配給装置は、前記データ提供装置から提供を受けた前記コンテンツファイル、あるいは前記管理装置から提供を受けた前記データ提供装置が提供したコンテンツデータに応じたコンテンツファイルを前記データ処理装置に配給し、前記データ処理装置は、前記データ配給装置あるいは前記管理装置から受けたキーファイルに格納された権利書データを復号し、当該復号した権利書データに基づいて、前記データ配給装置あるいは前記管理装置から受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定し、前記データ配給装置あるいは前記管理装置から受けた前記コンテンツファイルおよびキーファイルをさらに他のデータ処理装置に配信する。

【0069】

また、本発明の第1の観点のデータ提供方法は、データ提供装置からデータ処理装置にコンテンツデータを配給するデータ提供方法であって、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ提供装置から前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する。

【0070】

また、本発明の第2の観点のデータ提供方法は、データ提供装置からデータ処

理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記作成したキーファイルを前記管理装置から前記データ提供装置に配給し、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から配給を受けた前記キーファイルとを格納したモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ提供装置から前記データ処理装置に配給し、

前記データ処理装置において、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する。

【0071】

また、本発明の第3の観点のデータ提供方法は、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けたキーファイルとを含むコンテンツファイルを格納したモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する。

【0072】

また、本発明の第4の観点のデータ提供方法は、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置におい

て、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記管理装置から前記データ提供装置に配給し、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して個別に前記データ提供装置から前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

【 0 0 7 3 】

また、本発明の第 5 の観点のデータ提供方法は、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記管理装置から前記データ処理装置に配給し、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ提供装置から前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

【 0 0 7 4 】

また、本発明の第 6 の観点のデータ提供方法は、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置におい

て、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記キーファイルとを格納したモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する。

【0075】

また、本発明の第7の観点のデータ提供方法は、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記キーファイルとを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して個別に前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツデータの取り扱いを決定する。

【0076】

また、本発明の第8の観点のデータ提供方法は、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に配給し、前記データ提供装置において、前記

コンテンツ鍵データを用いて暗号化されたコンテンツデータを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツデータの取り扱いを決定する。

【0077】

また、本発明の第9の観点のデータ提供方法は、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを作成し、前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記暗号化されたコンテンツ鍵データおよび前記暗号化された権利書データとを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して個別に前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

【0078】

また、本発明の第10の観点のデータ提供方法は、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを作成して前記データ処理装置に配給し、前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた前記コンテンツ鍵データおよび前記権利書デ

ータを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツデータの取り扱いを決定する。

【0079】

また、本発明の第11の観点のデータ提供方法は、データ提供装置、データ配給装置およびデータ処理装置を用いたデータ提供方法であって、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納した第1のモジュールを前記データ提供装置から前記データ配給装置に提供し、前記提供を受けた前記第1のモジュールに格納された前記暗号化されたコンテンツデータ、コンテンツ鍵データおよび権利書データを格納した第2のモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ配給装置から前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた前記第2のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する。

【0080】

また、本発明の第12の観点のデータ提供方法は、データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記管理装置から前記データ提供装置に配給し、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとを格納した第1のモジュールを、前記データ提供装置から前記データ配給装置に提供し、前記提供を受けたコンテンツファイルおよび前記キーファイルを格納した第2のモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ配給装置から前記データ処理装置に配給

し、前記データ処理装置において、前記配給を受けた前記第2のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記第2のモジュールに格納された前記コンテンツデータの取り扱いを決定する。

【0081】

また、本発明の第13の観点のデータ提供方法は、データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと前記管理装置から受けたキーファイルとを含むコンテンツファイルを格納した第1のモジュールを前記データ配給装置に提供し、前記データ配給装置において、前記提供を受けたコンテンツファイルを格納した第2のモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた前記第2のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記第2のモジュールに格納された前記コンテンツデータの取り扱いを決定する。

【0082】

また、本発明の第14の観点のデータ提供方法は、データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供方法において、

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記作成したキーファイルを前記管理装置から前記データ提供装置に配給

し、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して個別に前記データ提供装置から前記データ配給装置に配給し、前記配給を受けた前記コンテンツファイルと前記キーファイルとを個別に前記データ配給装置から前記データ配給装置に配給し、前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

【 0 0 8 3 】

また、本発明の第 1 5 の観点のデータ提供方法は、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記管理装置から前記データ処理装置に配給し、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルを前記データ提供装置から前記データ配給装置に提供し、前記提供を受けたコンテンツファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ配給装置から前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

【 0 0 8 4 】

また、本発明の第 1 6 の観点のデータ提供方法は、データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供方法であって、前記

管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記キーファイルとを格納した第1のモジュールを前記データ配給装置に提供し、前記データ配給装置において、前記提供を受けたコンテンツデータおよび前記キーファイルを格納した第2のモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた前記第2のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記第2のモジュールに格納された前記コンテンツデータの取り扱いを決定する。

【0085】

また、本発明の第17の観点のデータ提供方法は、データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記キーファイルとを個別に前記データ配給装置に配給し、前記データ配給装置において、配給を受けた前記コンテンツデータと前記キーファイルとを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して個別に前記データ配給装置に配給し、前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツデータの取り扱いを決定する。

【0086】

また、本発明の第18の観点のデータ提供方法は、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に配給し、前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを前記データ配給装置に提供し、前記データ配給装置において、前記提供を受けたコンテンツデータを前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツデータの取り扱いを決定する。

【0087】

また、本発明の第19の観点のデータ提供方法は、データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを前記データ提供装置に提供し、前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記暗号化されたコンテンツ鍵データおよび前記暗号化された権利書データとを個別に前記データ配給装置に配給し、前記データ配給装置において、配給を受けた前記コンテンツデータと前記暗号化されたコンテンツ鍵データおよび前記暗号化された権利書データとを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して個別に前記データ配給装置に配給し、前記データ処理装置において、前記配給を受けた前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツデータの取り扱いを決定する。

【 0 0 8 8 】

また、本発明の第 2 0 の観点のデータ提供方法は、データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを前記データ処理装置に配給し、前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを前記データ配給装置に提供し、前記データ配給装置は、前記提供を受けたコンテンツデータを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツデータの取り扱いを決定する。

【 0 0 8 9 】

また、本発明の第 2 1 の観点のデータ提供方法は、データ提供装置、データ配給装置、管理装置およびデータ処理装置を用いたデータ提供方法であって、前記データ提供装置は、コンテンツのマスタソースデータを前記管理装置に提供し、前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置を管理し、前記提供されたマスタソースデータをコンテンツ鍵データを用いて暗号化してコンテンツデータを作成し、当該コンテンツデータを格納したコンテンツファイルを作成し、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記コンテンツファイルおよび前記キーファイルを前記データ配給装置に提供し、前記データ配給装置は、前記提供を受けた前記コンテンツファイルおよび前記キーファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書

データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

【0090】

また、本発明の第22の観点のデータ提供方法は、データ提供装置、データ配給装置、管理装置およびデータ処理装置を用いたデータ提供方法であって、前記データ提供装置は、コンテンツのマスタソースデータを前記管理装置に提供し、前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置を管理し、前記提供されたマスタソースデータをコンテンツ鍵データを用いて暗号化してコンテンツデータを作成し、当該コンテンツデータを格納したコンテンツファイルを作成し、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記コンテンツファイルを前記データ配給装置に提供し、前記キーファイルを前記データ処理装置に提供し、前記データ配給装置は、前記提供を受けた前記コンテンツファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

【0091】

また、本発明の第23の観点のデータ提供方法は、データ提供装置、データ配給装置、管理装置およびデータ処理装置を用いたデータ提供方法であって、前記データ提供装置は、コンテンツ鍵データを用いた暗号化したコンテンツデータを格納したコンテンツファイルを前記管理装置に提供し、前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置を管理し、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置から提供を受けた前記コンテンツファイルと、前記作成したキーファイルとを前記データ配給装置に提供し、前記データ配給装置は、前記提供を受けた前記コン

テンツファイルおよび前記キーファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

【 0 0 9 2 】

また、本発明の第 2 4 の観点のデータ提供方法は、データ提供装置、データ配給装置、管理装置およびデータ処理装置を用いたデータ提供方法であって、前記データ提供装置は、コンテンツ鍵データを用いた暗号化したコンテンツデータを格納したコンテンツファイルを前記管理装置に提供し、前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置を管理し、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置から提供を受けた前記コンテンツファイルを前記データ配給装置に提供し、前記作成したキーファイルを前記データ処理装置に提供し、前記データ配給装置は、前記提供を受けた前記コンテンツファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

【 0 0 9 3 】

また、本発明の第 2 5 の観点のデータ提供方法は、データ提供装置、データ配給装置、管理装置、データベース装置およびデータ処理装置を用いたデータ提供方法であって、前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルおよび前記管理装置から提供を受けたキーファイルを前記データベース装置に格納し、前記管理装置は、暗号化

された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ提供装置に提供し、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルおよびキーファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

【0094】

また、本発明の第26の観点のデータ提供方法は、データ提供装置、データ配給装置、管理装置、データベース装置およびデータ処理装置を用いたデータ提供方法であって、前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データベース装置に格納し、前記管理装置は、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ配給装置に提供し、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルと、前記データ配給装置から提供を受けたキーファイルとを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

【0095】

また、本発明の第27の観点のデータ提供方法は、データ提供装置、データ配給装置、管理装置、データベース装置およびデータ処理装置を用いたデータ提供方法であって、前記データ提供装置は、コンテンツ鍵データを用いてコンテンツ

データを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データベース装置に格納し、前記管理装置は、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に提供し、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

【0096】

また、本発明の第28の観点のデータ提供方法は、複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を用いたデータ提供方法であって、前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルおよび対応する前記管理装置から提供を受けたキーファイルを前記データベース装置に格納し、前記管理装置は、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを対応する前記データ提供装置に提供し、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルおよびキーファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

【 0 0 9 7 】

また、本発明の第 2 9 の観点のデータ提供方法は、複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を用いたデータ提供方法であって、前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データベース装置に格納し、前記管理装置は、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ配給装置に提供し、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルと、前記管理装置から提供を受けたキーファイルとを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

【 0 0 9 8 】

また、本発明の第 3 0 の観点のデータ提供方法は、複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を用いたデータ提供方法であって、前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データベース装置に格納し、前記管理装置は、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に提供し、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記

録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

【0099】

また、本発明の第31の観点のデータ提供方法は、複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を用いたデータ提供方法であって、前記データ提供装置は、コンテンツデータのマスターソースを対応する前記管理装置に提供し、当該管理装置から受けたコンテンツファイルおよびキーファイルを前記データベースに格納し、前記管理装置は、対応する前記データ提供装置から受けた前記マスターソースをコンテンツ鍵データを用いて暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記作成したコンテンツファイルおよび前記作成したキーファイルを対応する前記データ提供装置に送り、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルおよびキーファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

【0100】

また、本発明の第32の観点のデータ提供方法は、複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を用いたデータ提供方法であって、前記データ提供装置は、コンテンツデータのマスターソースを対応する前記管理装置に提供し、当該管理装置から受けたコンテンツファイルを前記データベースに格納し、前記管理装置は、対応する前記データ提供

装置から受けた前記マスソースをコンテンツ鍵データを用いて暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データ提供装置に送り、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを対応する前記データ配給装置に送り、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルと、前記管理装置から提供を受けたキーファイルとを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

【0101】

また、本発明の第33の観点のデータ提供方法は、複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を用いたデータ提供方法であって、前記データ提供装置は、コンテンツデータのマスソースを対応する前記管理装置に提供し、当該管理装置から受けたコンテンツファイルを前記データベースに格納し、前記管理装置は、対応する前記データ提供装置から受けた前記マスソースをコンテンツ鍵データを用いて暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データ提供装置に送り、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に提供し、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵

データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

【0102】

また、本発明の第34の観点のデータ提供方法は、データ提供装置、データ配給装置およびデータ処理装置を用いたデータ提供方法であって、前記データ提供装置は、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納した第1のモジュールを前記データ配給装置に提供し、前記データ処理装置から受けた履歴データに基づいて、コンテンツデータ単位で課金処理を行い、前記データ処理装置の関係者が支払った利益を当該データ提供装置の関係者と前記データ配給装置の関係者とに分配する利益分配処理を行い、前記データ配給装置は、前記提供を受けた前記第1のモジュールに格納された前記暗号化されたコンテンツデータ、コンテンツ鍵データおよび権利書データを格納した第2のモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定し、当該コンテンツデータの取り扱いについての履歴データを作成し、当該履歴データを前記データ提供装置に送る。

【0103】

また、本発明の第35の観点のデータ提供方法は、データ提供装置、データ配給装置、データ処理装置および管理装置を用いたデータ提供方法であって、前記データ提供装置は、コンテンツデータを提供し、前記データ配給装置は、前記データ提供装置から提供を受けた前記コンテンツファイル、あるいは前記管理装置から提供を受けた前記データ提供装置が提供したコンテンツデータに応じたコンテンツファイルを前記データ処理装置に配給し、前記データ処理装置は、前記データ配給装置あるいは前記管理装置から受けたキーファイルに格納された権利書

データを復号し、当該復号した権利書データに基づいて、前記データ配給装置あるいは前記管理装置から受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定し、前記データ配給装置あるいは前記管理装置から受けた前記コンテンツファイルおよびキーファイルをさらに他のデータ処理装置に配信する。

【0104】

また、本発明の第38の観点のデータ提供システムは、データ提供装置からデータ処理装置にコンテンツデータを配給するデータ提供システムであって、前記データ提供装置は、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを前記コンテンツデータの圧縮の有無、圧縮方式、前記暗号化の方式およびコンテンツデータを得た信号の諸元の少なくとも一つに依存しない形式で格納したモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する。

【0105】

また、本発明の第39の観点のデータ提供システムは、データ提供装置、データ配給装置およびデータ処理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを前記コンテンツデータの圧縮の有無、圧縮方式、前記暗号化の方式およびコンテンツデータを得た信号の諸元の少なくとも一つに依存しない形式で格納した第1のモジュールを前記データ配給装置に提供し、前記データ配給装置は、前記提供を受けた前記第1のモジュールに格納された前記暗号化されたコンテンツデータ、コンテンツ鍵データおよび権利書データを格納した第2のモジュールを、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいは記録媒体に記録して前記データ処理装置に配給

し、前記データ処理装置は、前記配給を受けた前記第 2 のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する。

【0106】

また、本発明の第 40 の観点のデータ提供システムは、データ提供装置、データ配給装置およびデータ処理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納した第 1 のモジュールを前記データ配給装置に提供し、前記データ配給装置は、前記提供を受けた前記第 1 のモジュールに格納された前記暗号化されたコンテンツデータ、コンテンツ鍵データおよび権利書データを格納した複数の第 2 のモジュールを、前記データ処理装置との間の相互認証によって得られた共有鍵を用いて暗号化した後に、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記複数の第 2 のモジュールを前記共有鍵を用いて復号し、当該復号した前記複数の第 2 のモジュールのなかから単数または複数の第 2 のモジュールを選択し、前記第 2 のモジュールの配給サービスに対しての課金処理を行う第 1 の処理回路と、前記選択された前記第 2 のモジュールを受けて当該第 2 のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する耐タンパ性の第 2 の処理回路とを有する。

【0107】

【発明の実施の形態】

以下、本発明の実施形態に係わる EMD (Electronic Music Distribution: 電子音楽配信) システムについて説明する。

第 1 実施形態

図 1 は、本実施形態の EMD システム 100 の構成図である。

本実施形態において、ユーザに配信されるコンテンツ (Content) データとは、情報そのものが価値を有するデジタルデータをいい、以下、音楽データ

を例に説明する。

図1に示すように、EMDシステム100は、コンテンツプロバイダ101、EMDサービスセンタ（クリアリング・ハウス、以下、ESCとも記す）102およびユーザホームネットワーク103を有する。

ここで、コンテンツプロバイダ101、EMDサービスセンタ102およびSAM105₁～105₄が、それぞれ請求項1および請求項6などに係るデータ提供装置、管理装置およびデータ処理装置に対応している。

先ず、EMDシステム100の概要について説明する。

EMDシステム100では、コンテンツプロバイダ101は、自らが提供しようとするコンテンツのコンテンツデータCを暗号化する際に用いたコンテンツ鍵データK_c、コンテンツデータCの使用許諾条件などの権利内容を示す権利書（UCP: Usage Control Policy）データ106、並びに電子透かし情報の内容および埋め込み位置を示す電子透かし情報管理データを、高い信頼性のある権威機関であるEMDサービスセンタ102に送る。

【0108】

EMDサービスセンタ102は、コンテンツプロバイダ101から受けたコンテンツ鍵データK_c、権利書データ106並びに電子透かし情報鍵データを登録（認証および権威化）する。

また、EMDサービスセンタ102は、対応する期間の配信用鍵データKD₁～KD₅₆で暗号化したコンテンツ鍵データK_c、権利書データ106および自らの署名データなどを格納したキーファイルKFを作成し、これをコンテンツプロバイダ101に送る。

ここで、当該署名データは、キーファイルKFの改竄の有無、キーファイルKFの作成者の正当性およびキーファイルKFがEMDサービスセンタ102において正規に登録されたことを検証するために用いられる。

【0109】

また、コンテンツプロバイダ101は、コンテンツ鍵データK_cでコンテンツデータCを暗号化してコンテンツファイルCFを生成し、当該生成したコンテンツファイルCFと、EMDサービスセンタ102から受けたキーファイルKFと

、自らの署名データなどを格納したセキュアコンテナ（本発明のモジュール）104を、インターネットなどのネットワーク、デジタル放送あるいは記録媒体などのパッケージメディアを用いて、ユーザホームネットワーク103に配給する。

ここで、セキュアコンテナ104内に格納された署名データは、対応するデータの改竄の有無、当該データの作成者および送信者の正当性を検証するために用いられる。

【0110】

ユーザホームネットワーク103は、例えば、ネットワーク機器160₁およびAV機器160₂～160₄を有する。

ネットワーク機器160₁は、SAM (Secure Application Module) 105₁を内蔵している。

AV機器160₂～160₄は、それぞれSAM105₂～105₄を内蔵している。SAM105₁～105₄相互間は、例えば、IEEE (Institute of Electrical and Electronics Engineers) 1394シリアルインタフェースバスなどのバス191を介して接続されている。

【0111】

SAM105₁～105₄は、ネットワーク機器160₁がコンテンツプロバイダ101からネットワークなどを介してオンラインで受信したセキュアコンテナ104、および／または、コンテンツプロバイダ101からAV機器160₂～160₄に記録媒体を介してオフラインで供給されたセキュアコンテナ104を対応する期間の配信用鍵データKD₁～KD₃を用いて復号した後に、署名データの検証を行う。

SAM105₁～105₄に供給されたセキュアコンテナ104は、ネットワーク機器160₁およびAV機器160₂～160₄において、ユーザの操作に応じて購入・利用形態が決定された後に、再生や記録媒体への記録などの対象となる。

SAM105₁～105₄は、上述したセキュアコンテナ104の購入・利用

の履歴を利用履歴 (Usage Log) データ 108 として記録すると共に、購入形態を示す利用制御状態データ 166 を作成する。

利用履歴データ 108 は、例えば、EMD サービスセンタ 102 からの要求に応じて、ユーザホームネットワーク 103 から EMD サービスセンタ 102 に送信される。

利用制御状態データ 166 は、例えば、購入形態が決定される度に、ユーザホームネットワーク 103 から EMD サービスセンタ 102 に送信される。

【0112】

EMD サービスセンタ 102 は、利用履歴データ 108 に基づいて、課金内容を決定 (計算) し、その結果に基づいて、ペイメントゲートウェイ 90 を介して銀行などの決済機関 91 に決済を行なう。これにより、ユーザホームネットワーク 103 のユーザが決済機関 91 に支払った金銭が、EMD サービスセンタ 102 による決済処理によって、コンテンツプロバイダ 101 に支払われる。

また、EMD サービスセンタ 102 は、一定期間毎に、決済レポートデータ 107 をコンテンツプロバイダ 101 に送信する。

【0113】

本実施形態では、EMD サービスセンタ 102 は、認証機能、鍵データ管理機能および権利処理 (利益分配) 機能を有している。

すなわち、EMD サービスセンタ 102 は、中立の立場にある最高の権威機関であるルート認証局 92 に対しての (ルート認証局 92 の下層に位置する) セカンド認証局 (Second Certificate Authority) としての役割を果たし、コンテンツプロバイダ 101 および SAM 105₁ ~ 105₄ において署名データの検証処理に用いられる公開鍵データの公開鍵証明書データに、EMD サービスセンタ 102 の秘密鍵データによる署名を付けることで、当該公開鍵データの正当性を認証する。また、前述したように、EMD サービスセンタ 102 は、コンテンツプロバイダ 101 の権利書データ 106 を登録して権威化することも、EMD サービスセンタ 102 の認証機能の一つである。

また、EMD サービスセンタ 102 は、例えば、配信用鍵データ KD₁ ~ KD₆ などの鍵データの管理を行なう鍵データ管理機能を有する。

また、EMDサービスセンタ102は、権威化した権利書データ106に記述された標準小売価格SRP (Suggested Retailer' Price) とSAM105₁～SAM105₄から入力した利用履歴データ108とに基づいて、ユーザによるコンテンツの購入・利用に対して決済を行い、ユーザが支払った金銭をコンテンツプロバイダ101に分配する権利処理(利益分配)機能を有する。

【0114】

図2は、セキュアコンテナ104の概念をまとめた図である。

図2に示すように、セキュアコンテナ104には、コンテンツプロバイダ101が作成したコンテンツファイルCFと、EMDサービスセンタ102が作成したキーファイルKFとが格納されている。

コンテンツファイルCFには、ヘッダ部およびコンテンツIDを含むヘッダデータと、コンテンツ鍵データK_cを用いた暗号化されたコンテンツデータCと、これらについてのコンテンツプロバイダ101の秘密鍵データK_{CP}, Sを用いた署名データとが格納されている。

キーファイルKFには、ヘッダ部およびコンテンツIDを含むヘッダデータと、配信用鍵データKD₁～KD₆によって暗号化されたコンテンツ鍵データK_cおよび権利書データ106と、これらについてのEMDサービスセンタ102の秘密鍵データK_{ESC}, Sによる署名データとが格納されている。

【0115】

以下、コンテンツプロバイダ101の各構成要素について詳細に説明する。

〔コンテンツプロバイダ101〕

図3は、コンテンツプロバイダ101の機能ブロック図であり、ユーザホームネットワーク103のSAM105₁～105₄との間で送受信されるデータに関連するデータの流れが示されている。

また、図4には、コンテンツプロバイダ101とEMDサービスセンタ102との間で送受信されるデータに関連するデータの流れが示されている。

なお、図4以降の図面では、署名データ処理部、および、セッション鍵データK_{SES}を用いた暗号化・復号部に入出力するデータの流れは省略している。

【0116】

図3および図4に示すように、コンテンツプロバイダ101は、コンテンツマスターソースデータベース111、電子透かし情報付加部112、圧縮部113、暗号化部114、乱数発生部115、伸長部116、署名処理部117、セキュアコンテナ作成部118、セキュアコンテナデータベース118a、キーファイルデータベース118b、記憶部（データベース）119、相互認証部120、暗号化・復号部121、権利書データ作成部122、聴感検査部123、SAM管理部124、EMDサービスセンタ管理部125およびコンテンツID生成部850を有する。

コンテンツプロバイダ101は、EMDサービスセンタ102との間で通信を行う前に、例えば、自らが生成した公開鍵データ、自らの身分証明書および銀行口座番号（決済を行う口座番号）をオフラインでEMDサービスセンタ102に登録し、自らの識別子（識別番号）CP_IDを得る。また、コンテンツプロバイダ101は、EMDサービスセンタ102から、EMDサービスセンタ102の公開鍵データと、ルート認証局92の公開鍵データとを受ける。

以下、図3および図4に示すコンテンツプロバイダ101の各機能ブロックについて説明する。

【0117】

コンテンツマスターソースデータベース111は、ユーザホームネットワーク103に提供するコンテンツのマスターソースであるコンテンツデータを記憶し、提供しようとするコンテンツデータS111を電子透かし情報付加部112に出力する。

【0118】

電子透かし情報付加部112は、コンテンツデータS111に対して、ソース電子透かし情報（Source Watermark）Ws、コピー管理用電子透かし情報（Copy Control Watermark）Wc、ユーザ電子透かし情報（User Watermark）Wuおよびリンク用電子透かし情報（Link Watermark）WLなどを埋め込んでコンテンツデータS112を生成し、コンテンツデータS112を圧縮部113に出力する。

【0119】

ソース電子透かし情報Wsは、コンテンツデータの著作権者名、ISRCコード、オーサリング日付、オーサリング機器ID (Identification Data)、コンテンツの配給先などの著作権に関する情報である。

コピー管理用電子透かし情報Wcは、アナログインタフェース経由でのコピー防止用のためのコピー禁止ビットを含む情報である。

ユーザ電子透かし情報Wuには、例えば、セキュアコンテナ104の配給元および配給先を特定するためのコンテンツプロバイダ101の識別子CP_IDおよびユーザホームネットワーク103のSAM105₁~105₄の識別子SAM_ID₁~SAM_ID₄が含まれる。

リンク用電子透かし情報(Link Watermark)WLは、例えば、コンテンツデータCのコンテンツIDを含んでいる。

リンク用電子透かし情報WLをコンテンツデータCに埋め込むことで、例えば、テレビジョンやAM/FMラジオなどのアナログ放送でコンテンツデータCが配信された場合でも、ユーザからの要求に応じて、EMDサービスセンタ102は、当該コンテンツデータCを扱っているコンテンツプロバイダ101をユーザに紹介できる。すなち、当該コンテンツデータCの受信先において、電子透かし情報デコーダを利用したコンテンツデータCに埋め込まれたリンク用電子透かし情報WLを検出し、当該検出したリンク用電子透かし情報WLに含まれるコンテンツIDをEMDサービスセンタ102に送信することで、EMDサービスセンタ102は当該ユーザに対して、当該コンテンツデータCを扱っているコンテンツプロバイダ101などを紹介できる。

【0120】

具体的には、例えば、車の中でユーザがラジオを聞きながら、放送中の曲が良いとユーザが思った時点で、所定のボタンを押せば、当該ラジオに内蔵されている電子透かし情報デコーダが、当該コンテンツデータCに埋め込まれているリンク用電子透かし情報WLに含まれるコンテンツIDや当該コンテンツデータCを登録しているEMDサービスセンタ102の通信アドレスなどを検出し、当該検出したデータをメモリスティックなどの半導体メモリやMD (Mini Dis

k) などの光ディスクなどの可搬メディアに搭載されているメディアSAMに記録する。そして、当該可搬メディアをネットワークに接続されているSAMを搭載したネットワーク機器をセットする。そして、当該SAMとEMDサービスセンタ102とが相互認証を行った後に、メディアSAMに搭載されている個人情報と、上記記録したコンテンツIDなどをネットワーク機器からEMDサービスセンタ102に送信する。その後、ネットワーク機器に、当該コンテンツデータCを扱っているコンテンツプロバイダ101などの紹介リストなどを、EMDサービスセンタ102から受信する。

また、その他に、例えば、EMDサービスセンタ102が、ユーザからコンテンツIDなどを受信したときに、当該コンテンツIDに対応したコンテンツデータCを提供しているコンテンツプロバイダ101に当該ユーザを特定した情報を通知してもよい。この場合に、当該通信を受けたコンテンツプロバイダ101は、当該ユーザが契約者であれば、当該コンテンツデータCをユーザのネットワーク機器に送信し、当該ユーザが契約者でなければ、自らに関するプロモーション情報をユーザのネットワーク機器に送信してもよい。

【0121】

なお、後述する第2実施形態では、リンク用電子透かし情報WLに基づいて、EMDサービスセンタ302は、ユーザに、当該コンテンツデータCを扱っているサービスプロバイダ310を紹介できる。

【0122】

また、本実施形態では、好ましくは、各々の電子透かし情報の内容と埋め込み位置とを、電子透かし情報モジュールWMとして定義し、EMDサービスセンタ102において電子透かし情報モジュールWMを登録して管理する。電子透かし情報モジュールWMは、例えば、ユーザホームネットワーク103内のネットワーク機器160₁およびAV機器160₂～160₄が、電子透かし情報の正当性を検証する際に用いられる。

例えば、ユーザホームネットワーク103では、EMDサービスセンタ102が管理するユーザ電子透かし情報モジュールに基づいて、電子透かし情報の埋め込み位置および埋め込まれた電子透かし情報の内容の双方が一致した場合に電子

透かし情報が正当であると判断することで、偽りの電子透かし情報の埋め込みを高い確率で検出できる。

【0123】

圧縮部113は、コンテンツデータS112を、例えば、ATRAC3 (Adaptive Transform Acoustic Coding 3) (商標)などの音声圧縮方式で圧縮し、圧縮したコンテンツデータS113を暗号化部114に出力する。

この場合に、圧縮部113による圧縮時に、コンテンツデータに対しての電子透かし情報の埋め込みを再び行ってもよい。具体的には、図3に示すように、伸長部116においてコンテンツデータ113を伸長してコンテンツデータS116を生成し、聴感検査部123においてコンテンツデータS116を再生したときに、電子透かし情報の埋め込みが音質に与える影響を、例えば実際に人間が聴いて判断し、所定の基準を満たさない場合には、電子透かし情報付加部112に電子透かし情報の埋め込み処理を再び行うように指示する。

これにより、例えば、データの損失を伴う音声圧縮方式を採用したときに、当該圧縮によって、埋め込んだ電子透かし情報が落ちてしまった場合に適切に対処できる。また、圧縮したコンテンツデータを再度伸長して、埋め込みを行った電子透かし情報を正確に検出できるか否かの確認を行ってもよい。この場合に、音質聴感の検証も行い、聴感上問題がある場合には、電子透かし情報の埋め込みの調整を行う。例えば、マスキング効果を利用して電子透かし情報を埋め込む場合には、電子透かし情報の埋め込みを行うレベルを調整する。

【0124】

暗号化部114は、コンテンツ鍵データKcを共通鍵として用い、DES (Data Encryption Standard) やTriple DESなどの共通鍵暗号化方式で、コンテンツデータS113を暗号化してコンテンツデータCを生成し、これをセキュアコンテナ作成部118に出力する。

また、暗号化部114は、コンテンツ鍵データKcを共通鍵として用い、A/V伸長用ソフトウェアSoft、メタデータMetaおよび電子透かし情報管理データWMを暗号化した後に、セキュアコンテナ作成部117に出力する。

【0125】

DESは、56ビットの共通鍵を用い、平文の64ビットを1ブロックとして処理する暗号化方式である。DESの処理は、平文を攪拌し、暗号文に変換する部分（データ攪拌部）と、データ攪拌部で使用する鍵（拡大鍵）データを共通鍵データから生成する部分（鍵処理部）とからなる。DESの全てのアルゴリズムは公開されているので、ここでは、データ攪拌部の基本的な処理を簡単に説明する。

【0126】

先ず、平文の64ビットは、上位32ビットの H_0 と下位32ビットの L_0 とに分割される。鍵処理部から供給された48ビットの拡大鍵データ K_1 および下位32ビットの L_0 を入力とし、下位32ビットの L_0 を攪拌したF関数の出力が算出される。F関数は、数値を所定の規則で置き換える「換字」およびビット位置を所定の規則で入れ替える「転置」の2種類の基本変換から構成されている。次に、上位32ビットの H_0 と、F関数の出力との排他的論理和が算出され、その結果は L_1 とされる。また、 L_0 は、 H_1 とされる。

そして、上位32ビットの H_0 および下位32ビットの L_0 を基に、以上の処理を16回繰り返し、得られた上位32ビットの H_{16} および下位32ビットの L_{16} が暗号文として出力される。復号は、暗号化に使用した共通鍵データを用いて、上記の手順を逆さにたどることで実現される。

【0127】

乱数発生部115は、所定ビット数の乱数を発生し、当該乱数をコンテンツ鍵データ K_c として記憶部119に記憶する。

なお、コンテンツ鍵データ K_c は、コンテンツデータが提供する楽曲に関する情報から生成してもよい。コンテンツ鍵データ K_c は、例えば、所定時間毎に更新される。

また、複数のコンテンツプロバイダ101が存在する場合に、個々のコンテンツプロバイダ101によって固有のコンテンツ鍵データ K_c を用いてもよいし、全てのコンテンツプロバイダ101に共通のコンテンツ鍵データ K_c を用いてもよい。

【0128】

キーファイルデータベース 118b には、図 4 に示すように、EMD サービスセンタ管理部 125 を介して EMD サービスセンタ 102 から受信した図 5 (B) に示すキーファイル KF が記憶される。キーファイル KF は、コンテンツデータ C 毎に存在し、後述するように、コンテンツファイル CF のヘッダ内のディレクトリ構造データ DSD によって、対応するコンテンツファイル CF との間でリンク関係が指定されている。

キーファイル KF には、図 5 (B) および図 7 に示すように、ヘッダ、コンテンツ鍵データ Kc、権利書データ (使用許諾条件) 106、SAM プログラム・ダウンロード・コンテナ SDC₁ ~ SDC₃ および署名データ SIG_{K1}, ESC_C が格納されている。

ここで、コンテンツプロバイダ 101 の秘密鍵データ K_{ESC, S} を用いた署名データは、図 5 (B) に示すようにキーファイル KF に格納される全てのデータに対しての署名データ K₁, ESC にしてもよいし、図 7 に示すようにヘッダから鍵ファイルに関する情報までのデータに対しての署名データと、コンテンツ鍵データ Kc および権利書データ 106 に対しての署名データと、SAM プログラム・ダウンロード・コンテナ SDC に対しての署名データとを別々に設けてもよい。

コンテンツ鍵データ Kc および権利書データ 106 と、SAM プログラム・ダウンロード・コンテナ SDC₁ ~ SDC₃ とは、それぞれ対応する期間の配信用鍵データ KD₁ ~ KD₆ を用いて暗号化されている。

【0129】

ヘッダデータには、図 7 に示すように、同期信号、コンテンツ ID、コンテンツ ID に対してのコンテンツプロバイダ 101 の秘密鍵データ K_{ESC, S} による署名データ、ディレクトリ構造データ、ハイパーリンクデータ、キーファイル KF に関する情報、およびディレクトリ構造データ等に対してのコンテンツプロバイダ 101 の秘密鍵データ K_{ESC, S} による署名データが含まれる。

なお、ヘッダデータに含める情報としては種々の情報が考えられ、状況に応じて任意に変更可能である。例えば、ヘッダデータに、図 8 に示すような情報を含

めてもよい。

また、コンテンツIDには、例えば、図9に示す情報が含まれている。コンテンツIDは、EMDサービスセンタ102あるいはコンテンツプロバイダ101において作成され、EMDサービスセンタ102において作成された場合には図9に示すようにEMDサービスセンタ102の秘密鍵データ $K_{ESC, S}$ による署名データが添付され、コンテンツプロバイダ101において作成された場合にはコンテンツプロバイダ101の秘密鍵データ $K_{CP, S}$ が添付される。

コンテンツIDは、例えば、図4に示すように、コンテンツID生成部850が作成し、記憶部119に格納される。なお、コンテンツIDは、EMDサービスセンタ102が作成してもよい。

【0130】

ディレクトリ構造データは、セキュアコンテナ104内におけるコンテンツファイルCF相互間の対応関係と、コンテンツファイルCFとキーファイルKFとの対応関係を示している。

例えば、セキュアコンテナ104内にコンテンツファイル $CF_1 \sim CF_3$ と、それらに対応するキーファイル $KF_1 \sim KF_3$ が格納されている場合には、図10に示すように、コンテンツファイル $CF_1 \sim CF_3$ 相互間のリンクと、コンテンツファイル $CF_1 \sim CF_3$ とキーファイル $KF_1 \sim KF_3$ との間のリンク関係とがディレクトリ構造データによって確立される。

ハイパーリンクデータは、セキュアコンテナ104の内外の全てのファイルを対象として、キーファイルKF相互間での階層構造と、コンテンツファイルCFとキーファイルKFとの対応関係を示している。

具体的には、図11に示すように、セキュアコンテナ104内にコンテンツファイルCFおよびキーファイルKF毎のリンク先のアドレス情報とその認証値（ハッシュ値）とを格納し、ハッシュ関数 $H(x)$ を用いて得た自らのアドレス情報のハッシュ値と、相手方の認証値とを比較してリンク関係を検証する。

【0131】

また、権利書データ106には、図7に示すように、コンテンツID、コンテンツプロバイダ101の識別子 CP_ID 、権利書データ106の有効期限、E

MDサービスセンタ102の通信アドレス、利用空間調査情報、卸売価格情報、取扱方針、取扱制御情報、商品デモ（試聴）の取扱制御情報およびそれらについての署名データなどが含まれる。

なお、後述する第2実施形態のように、サービスプロバイダ310を介してユーザホームネットワーク303にセキュアコンテナ304を送信する場合には、権利書データ106には、コンテンツプロバイダ301がセキュアコンテナ104を提供するサービスプロバイダ310の識別子SP_IDが含まれる。

【0132】

また、SAMプログラム・ダウンロード・コンテナSDC₁～SDC₃には、図7に示すように、SAM105₁～105₄内でプログラムのダウンロードを行なう際に用いられるダウンロードの手順を示すダウンロード・ドライバと、権利書データ（UCP）U106のシンタックス（文法）を示すUCP-L（Label）. R（Reader）などのラベルリーダと、SAM105₁～105₄に内蔵された記憶部（フラッシュROM）の書き換えおよび消去をブロック単位でロック状態／非ロック状態にするためのロック鍵データと、それらについての署名データとが含まれる。

【0133】

なお、記憶部119は、例えば、公開鍵証明書データを記憶するデータベースを含む種々のデータベースを備えている。

【0134】

署名処理部117は、署名を行なう対象となるデータのハッシュ値をとり、コンテンツプロバイダ101の秘密鍵データK_{CP, S}を用いて、その署名データSIGを作成する。

【0135】

なお、ハッシュ値は、ハッシュ関数を用いて生成される。ハッシュ関数は、対象となるデータを入力とし、当該入力したデータを所定のビット長のデータに圧縮し、ハッシュ値として出力する関数である。ハッシュ関数は、ハッシュ値（出力）から入力を予測することが難しく、ハッシュ関数に入力されたデータの1ビットが変化したとき、ハッシュ値の多くのビットが変化し、また、同一のハッシ

ュ値を持つ入力データを探し出すことが困難であるという特徴を有している。

【0136】

セキュアコンテナ作成部118は、図5(A)に示すように、ヘッダデータと、暗号化部114から入力したそれぞれコンテンツ鍵データ K_c で暗号化されたメタデータ $Meta$ 、コンテンツデータ C 、A/V伸長用ソフトウェア $Soft$ および電子透かし情報モジュール(Watermark Module)WMとを格納したコンテンツファイル CF を生成する。

【0137】

コンテンツファイル CF には、図6に示すように、ファイルリーダと、秘密鍵データ $K_{cp, S}$ によるファイルリーダの署名データとを含むようにしてもよい。このようにすることで、 $SAM105_1 \sim 105_4$ において、異系列の複数のセキュアコンテナ104から受信したそれぞれ異なるフォーマットのコンテンツファイル CF を格納した複数のセキュアコンテナ104を効率的に処理できる。

【0138】

ここで、ファイルリーダは、コンテンツファイル CF およびそれに対応するキーファイル KF を読む際に用いられ、これらのファイルの読み込み手順などを示している。

但し、本実施形態では、EMDサービスセンタ102から $SAM105_1 \sim 105_4$ に、当該ファイルリーダを予め送信している場合を例示する。すなわち、本実施形態では、セキュアコンテナ104のコンテンツファイル CF は、ファイルリーダを格納していない。

【0139】

ヘッダデータには、図6に示すように、同期信号、コンテンツID、コンテンツIDに対してのコンテンツプロバイダ101の秘密鍵データ $K_{CP, S}$ による署名データ、ディレクトリ情報、ハイパーリンク情報、シリアルナンバー、コンテンツファイル CF の有効期限並びに作成者情報、ファイルサイズ、暗号の有無、暗号アルゴリズム、署名アルゴリズムに関する情報、およびディレクトリ情報などに関するコンテンツプロバイダ101の秘密鍵データ $K_{CP, S}$ による署名データが含まれる。

【0140】

メタデータMetaには、図6に示すように、商品（コンテンツデータC）の説明文、商品デモ宣伝情報、商品関連情報およびこれらについてのコンテンツプロバイダ101による署名データが含まれる。

本発明では、図5および図6に示すように、コンテンツファイルCF内にメタデータMetaを格納して送信する場合を例示するが、メタデータMetaをコンテンツファイルCF内に格納せずに、コンテンツファイルCFを送信する経路とは別の経路でコンテンツプロバイダ101からSAM105₁などに送信してもよい。

【0141】

A/V伸長用ソフトウェアSoftは、ユーザホームネットワーク103のネットワーク機器160₁およびAV機器160₂～160₄において、コンテンツファイルCFを伸長する際に用いられるソフトウェアであり、例えば、ATRAC3方式の伸長用ソフトウェアである。

このように、セキュアコンテナ104内にA/V伸長用ソフトウェアSoftを格納することで、SAM105₁～105₄においてセキュアコンテナ104内に格納されたA/V伸長用ソフトウェアSoftを用いてコンテンツデータCの伸長を行うことができ、コンテンツデータC毎あるいはコンテンツプロバイダ101毎にコンテンツデータCの圧縮および伸長方式をコンテンツプロバイダ101が自由に設定しても、ユーザに多大な負担をかけることはない。

【0142】

電子透かし情報モジュールWMは、前述したように、例えば、コンテンツデータCに埋め込まれた電子透かし情報を検出するのに必要な情報およびソフトウェアを含んでいる。

【0143】

また、セキュアコンテナ作成部118は、上述した図5（A）に示すコンテンツファイルCFと、当該コンテンツファイルCFの署名データSIG₆、CPと、キーファイルデータベース118bから読み出した当該コンテンツファイルCFに対応する図5（B）に示すキーファイルKFと、当該キーファイルKFの署

名データSIG₇, CPと、記憶部119から読み出したコンテンツプロバイダ101の公開鍵証明書データCER_{CP}と、当該公開鍵証明書データCER_{CP}の署名データSIG₁, ESCとを格納したセキュアコンテナ104を生成する。

【0144】

ここで、署名データSIG₆, CPは、セキュアコンテナ104の受信先において、コンテンツファイルCFの作成者および送信者の正当性を検証するために用いられる。

ここで、署名データSIG₇, CPは、セキュアコンテナ104の受信先において、キーファイルKFの送信者の正当性を検証するために用いられる。なお、セキュアコンテナ104の受信先において、キーファイルKFの作成者の正当性の検証は、キーファイルKF内の署名データSIG_{K1}, ESCに基づいて行われる。また、署名データSIG_{K1}, ESCは、キーファイルKFが、EMDサービスセンタ102に登録されているか否かを検証するためにも用いられる。

【0145】

本実施形態では、コンテンツデータCの圧縮方式、圧縮の有無、暗号化方式（共通鍵暗号化方式および公開鍵暗号化方式の何れの場合も含む）、コンテンツデータCを得た信号の諸元（サンプリング周波数など）および署名データの作成方式（アルゴリズム）に依存しない形式で、暗号化されたコンテンツデータCがセキュアコンテナ104内に格納されている。すなわち、これらの事項をコンテンツプロバイダ101が自由に決定できる。

【0146】

また、セキュアコンテナ作成部118は、セキュアコンテナデータバス118aに格納したセキュアコンテナ104を、ユーザからの要求に応じてSAM管理部124に出力する。

このように、本実施形態では、コンテンツプロバイダ101の公開鍵データKCP, Pの公開鍵証明書CER_{CP}をセキュアコンテナ104に格納してユーザホームネットワーク103に送信するイン・バンド（In-band）方式を採用している。従って、ユーザホームネットワーク103は、公開鍵証明書CER

C_P を得るための通信をEMDサービスセンタ102との間で行う必要がない。

なお、本発明では、公開鍵証明書 CER_{C_P} をセキュアコンテナ104に格納しないで、ユーザホームネットワーク103がEMDサービスセンタ102から公開鍵証明書 CER_{C_P} を得るアウト・オブ・バンド (Out-Of-band) 方式を採用してもよい。

【0147】

相互認証部120は、コンテンツプロバイダ101がEMDサービスセンタ102およびユーザホームネットワーク103との間でオンラインでデータを送受信する際に、それぞれEMDサービスセンタ102およびユーザホームネットワーク103との間で相互認証を行ってセッション鍵データ (共有鍵) K_{SES} を生成する。セッション鍵データ K_{SES} は、相互認証を行う度に新たに生成される。

【0148】

暗号化・復号部121は、コンテンツプロバイダ101がEMDサービスセンタ102およびユーザホームネットワーク103にオンラインで送信するデータを、セッション鍵データ K_{SES} を用いて暗号化する。

また、暗号化・復号部121は、コンテンツプロバイダ101がEMDサービスセンタ102およびユーザホームネットワーク103からオンラインで受信したデータを、セッション鍵データ K_{SES} を用いて復号する。

【0149】

権利書データ作成部122は、権利書データ106を作成し、これをEMDサービスセンタ管理部125に出力する。

権利書データ106は、コンテンツデータCの運用ルールを定義した記述子 (ディスクリプター) であり、例えば、コンテンツプロバイダ101の運用者が希望する標準小売価格SRP (Suggested Retailer's Price) やコンテンツデータCの複製ルールなどが記述されている。

【0150】

SAM管理部124は、セキュアコンテナ104を、オフラインおよび／またはオンラインでユーザホームネットワーク103に供給する。

また、SAM管理部 124 は、セキュアコンテナ 104 をオンラインで SAM 105₁ ~ 105₄ に配給する場合には、セキュアコンテナ 104 を送信する通信プロトコルとして、デジタル放送であれば MHEG (Multimedia and Hypermedia information coding Experts Group) プロトコルを用い、インターネットであれば XML/SMIL/HTML (Hyper Text Markup Language) を用い、これらの通信プロトコル内に、セキュアコンテナ 104 を、符号化方式に依存しない形式でトンネリングして埋め込む。

従って、通信プロトコルとセキュアコンテナ 104 との間でフォーマットの整合性をとる必要性はなく、セキュアコンテナ 104 のフォーマットを柔軟に設定できる。

なお、コンテンツプロバイダ 101 からユーザホームネットワーク 103 にセキュアコンテナ 104 を送信する際に用いる通信プロトコルは、上述したものには限定されず任意である。

【0151】

図 12 は、本実施形態で用いられる ROM 型の記録媒体 130₁ を説明するための図である。

図 12 に示すように、ROM 型の記録媒体 130₁ は、ROM 領域 131、セキュア RAM 領域 132 およびメディア SAM 133 を有する。

ROM 領域 131 には、図 5 (A) に示したコンテンツファイル CF が記憶されている。

また、セキュア RAM 領域 132 は、記憶データに対してのアクセスに所定の許可 (認証) が必要な領域であり、図 5 (B)、(C) に示したキーファイル KF および公開鍵証明書データ CER_{CP} と機器の種類に応じて固有の値を持つ記録用鍵データ K_{STR} とを引数として MAC (Message Authentication Code) 関数を用いて生成した署名データと、当該キーファイル KF および公開鍵証明書データ CER_{CP} とを記録媒体に固有の値を持つメディア鍵データ K_{MED} を用いて暗号化したデータとが記憶される。

また、セキュア RAM 領域 132 には、例えば、不正行為などで無効となった

コンテンツプロバイダ 101 および SAM 105₁ ~ 105₅ を特定する公開鍵証明書破棄データ（リボケーションリスト）が記憶される。

また、セキュア RAM 領域 132 には、後述するようにユーザホームネットワーク 103 の SAM 105₁ ~ 105₄ においてコンテンツデータ C の購入・利用形態が決定されたときに生成される利用制御状態（UCS）データ 166 などが記憶される。これにより、利用制御状態データ 166 がセキュア RAM 領域 132 に記憶されることで、購入・利用形態が決定した ROM 型の記録媒体 130₁ となる。

メディア SAM 133 には、例えば、ROM 型の記録媒体 130₁ の識別子であるメディア ID と、メディア鍵データ K_{MED} とが記憶されている。

メディア SAM 133 は、例えば、相互認証機能を有している。

【0152】

本実施形態で用いる ROM 型の記録媒体としては、例えば、図 12 に示すものの他に、図 13 に示す ROM 型の記録媒体 130₂ および図 14 に示す ROM 型の記録媒体 130₃ なども考えられる。

図 13 に示す ROM 型の記録媒体 130₂ は、ROM 領域 131 と認証機能を有するメディア SAM 133 とを有し、図 12 に示す ROM 型の記録媒体 130₁ のようにセキュア RAM 領域 132 を備えていない。ROM 型の記録媒体 130₂ を用いる場合には、ROM 領域 131 にコンテンツファイル CF を記録し、メディア SAM 133 にキーファイル KF を記憶する。

また、図 14 に示す ROM 型の記録媒体 130₃ は、ROM 領域 131 およびセキュア RAM 領域 132 を有し、図 12 に示す ROM 型の記録媒体 130₁ のようにメディア SAM 133 を有していない。ROM 型の記録媒体 130₃ を用いる場合には、ROM 領域 131 にコンテンツファイル CF を記録し、セキュア RAM 領域 132 にキーファイル KF を記録する。また、ROM 型の記録媒体 130₃ を用いる場合には、SAM との間で相互認証は行わない。

また、本実施形態では ROM 型の記録媒体の他に RAM 型の記録媒体も用いられる。

【0153】

本実施形態で用いるRAM型の記録媒体としては、例えば図15に示すように、メディアSAM133、セキュアRAM領域132およびセキュアでないRAM領域134を有するRAM型の記録媒体130₄がある。RAM型の記録媒体130₄では、メディアSAM133は認証機能を持ち、キーファイルKFを記憶する。また、RAM領域134には、コンテンツファイルCFが記録される。

また、本実施形態で用いるRAM型の記録媒体としては、その他に、図16に示すRAM型の記録媒体1350₅および図17に示すRAM型の記録媒体130₆なども考えられる。

図16に示すRAM型の記録媒体130₅は、セキュアでないRAM領域134と認証機能を有するメディアSAM133とを有し、図15に示すRAM型の記録媒体130₄のようにセキュアRAM領域132を備えていない。RAM型の記録媒体130₅を用いる場合には、RAM領域134にコンテンツファイルCFを記録し、メディアSAM133にキーファイルKFを記憶する。

また、図17に示すRAM型の記録媒体130₆は、セキュアRAM領域132およびセキュアでないRAM領域134を有し、図15に示すRAM型の記録媒体130₄のようにメディアSAM133を有していない。RAM型の記録媒体130₆を用いる場合には、RAM領域134にコンテンツファイルCFを記録し、セキュアRAM領域132にキーファイルKFを記録する。また、RAM型の記録媒体130₆を用いる場合には、SAMとの間で相互認証は行わない。

【0154】

また、SAM管理部124は、セキュアコンテナ104を、ネットワークやデジタル放送などを用いてオンラインでユーザホームネットワーク103に配信する場合には、暗号化・復号部121においてセッション鍵データK_{SES}を用いてセキュアコンテナ104を暗号化した後に、ネットワークを介してユーザホームネットワーク103に配信する。

本実施形態では、SAM管理部、EMDサービスセンタ管理部、並びに後述するコンテンツプロバイダ管理部およびサービスプロバイダ管理部として、例えば、内部の処理内容の監視（モニタリング）および改竄ができないあるいは困難な耐タンパ性の構造を持つ通信ゲートウェイが用いられる。

【0155】

ここで、コンテンツプロバイダ101からユーザホームネットワーク103へのコンテンツデータCの配給は、上述したように記録媒体130₁を用いて行う場合とネットワークを使ってオンラインで行う場合との何れでも権利書データ106が格納された共通の形式のセキュアコンテナ104を用いる。従って、ユーザホームネットワーク103のSAM105₁～105₄では、オフラインおよびオンラインの何れの場合でも、共通の権利書データ106に基づいた権利処理を行なうことができる。

【0156】

また、上述したように、本実施形態では、セキュアコンテナ104内に、コンテンツ鍵データK_cで暗号化されたコンテンツデータCと、当該暗号化を解くためのコンテンツ鍵データK_cとを同封するイン・バンド(In-Band)方式を採用している。イン・バンド方式では、ユーザホームネットワーク103の機器で、コンテンツデータCを再生しようとするときに、コンテンツ鍵データK_cを別途配信する必要がなく、ネットワーク通信の負荷を軽減できるという利点がある。また、コンテンツ鍵データK_cは配信用鍵データKD₁～KD₆で暗号化されているが、配信用鍵データKD₁～KD₆は、EMDサービスセンタ102で管理されており、ユーザホームネットワーク103のSAM105₁～105₅に事前に(SAM105₁～105₄がEMDサービスセンタ102に初回にアクセスする際に)配信されているので、ユーザホームネットワーク103では、EMDサービスセンタ102との間をオンラインで接続することなく、オフラインで、コンテンツデータCの利用が可能になる。

なお、本発明は、後述するようにコンテンツデータCとコンテンツ鍵データK_cとを別々に、ユーザホームネットワーク103に供給するアウト・オブ・バンド(Out-Of-Band)方式を採用できる柔軟性を有している。

【0157】

EMDサービスセンタ管理部125は、EMDサービスセンタ102から決済レポートデータ107を受信すると、これらを暗号化・復号部121においてセッション鍵データK_{SES}を用いて復号した後に、記憶部119に記憶する。

決済レポートデータ107は、例えば、EMDサービスセンタ102が図1に示す決済機関91に対して行なったコンテンツプロバイダ101に関する決済の内容が記述されている。

【0158】

また、EMDサービスセンタ管理部125は、提供するコンテンツデータCのグローバルユニーク (Global Unique) な識別子であるコンテンツID、公開鍵データ $K_{CP, P}$ およびそれらの署名データ $SIG_{g, CP}$ を、EMDサービスセンタ102に送信し、EMDサービスセンタ102から、公開鍵データ $K_{CP, P}$ の公開鍵証明書データ CER_{CP} を入力する。

また、EMDサービスセンタ管理部125は、コンテンツデータCのそれぞれについて、コンテンツ鍵データ K_c 、権利書データ106および電子透かし情報管理データWMをEMDサービスセンタ102に登録してキーファイルKFを受け取る際に、図18に示すように、提供するコンテンツデータCのグローバルユニークな識別子であるコンテンツID、コンテンツ鍵データ K_c 、権利書データ106、電子透かし情報管理データWM、コンテンツプロバイダ101のグローバルユニークな識別子である CP_ID と、それらについてのコンテンツプロバイダ101の秘密鍵データ $K_{CP, S}$ による署名データ $SIG_{M1, CP}$ とを格納した登録モジュール Mod_2 を作成する。そして、EMDサービスセンタ管理部125は、登録モジュール Mod_2 を暗号化・復号部121においてセッション鍵データ K_{SES} を用いて暗号化した後に、ネットワークを介してEMDサービスセンタ102に送信する。EMDサービスセンタ管理部125としては、前述したように、例えば、内部の処理内容の監視（モニタリング）および改竄ができないあるいは困難な耐タンパ性の構造を持つ通信ゲートウェイが用いられる。

【0159】

以下、図3および図4を参照しながら、コンテンツプロバイダ101における処理の流れを説明する。

なお、以下に示す処理を行う前提として、コンテンツプロバイダ101の関係者は、例えば、自らの身分証明書および決済処理を行う銀行口座などを用いて、オフラインで、EMDサービスセンタ102に登録処理を行い、グローバルユニ

ークな識別子 CP_ID を得ている。識別子 CP_ID は、記憶部 119 に記憶されている。

【0160】

先ず、コンテンツプロバイダ 101 が、EMD サービスセンタ 102 に、自らの秘密鍵データ $K_{CP, S}$ に対応する公開鍵データ $K_{CP, S}$ の正当性を証明する公開鍵証明書データ CER_{CP} を要求する場合の処理を図 4 を参照しながら説明する。

コンテンツプロバイダ 101 は、真性乱数発生器を用いて乱数を発生して秘密鍵データ $K_{CP, S}$ を生成し、当該秘密鍵データ $K_{CP, S}$ に対応する公開鍵データ $K_{CP, P}$ を作成して記憶部 119 に記憶する。

EMD サービスセンタ管理部 125 は、コンテンツプロバイダ 101 の識別子 CP_ID および公開鍵データ $K_{CP, P}$ を記憶部 119 から読み出す。

そして、EMD サービスセンタ管理部 125 は、識別子 CP_ID および公開鍵データ $K_{CP, P}$ を、EMD サービスセンタ 102 に送信する。

そして、EMD サービスセンタ管理部 125 は、当該登録に応じて、公開鍵証明書データ CER_{CP} およびその署名データ SIG_1, ESC を EMD サービスセンタ 102 から入力して記憶部 119 に書き込む。

【0161】

次に、コンテンツプロバイダ 101 が、EMD サービスセンタ 102 にコンテンツ鍵データ K_c 、権利書データ 106 および電子透かし情報管理データ WM を登録し、コンテンツデータ C に対応するキーファイル KF を受信する場合の処理を図 4、図 18 および図 19 を参照して説明する。

権利書データ 106 などの登録は、個々のコンテンツデータ C についてそれぞれ行われる。

図 19 は、コンテンツプロバイダ 101 から EMD サービスセンタ 102 への登録処理を説明するためのフローチャートである。

【0162】

ステップ A1：図 4 に示すコンテンツプロバイダ 101 の相互認証部 120 と EMD サービスセンタ 102 との間で相互認証を行う。

ステップA2：ステップA1で行った相互認証によって得られたセッション鍵データ K_{SES} をコンテンツプロバイダ101およびEMDサービスセンタ102で共有する。

【0163】

ステップA3：コンテンツプロバイダ101は、記憶部119などのデータベースから、EMDサービスセンタ102に登録を行うコンテンツID、コンテンツ鍵データ K_c 、権利書データ106、電子透かし情報管理データWMおよびCP_IDなどを読み出す。

ステップA4：署名処理部117において、コンテンツプロバイダ101の秘密鍵データ $K_{CP, S}$ を用いて、ステップA3で読み出した権利書データ106などを含むモジュールに対して、送り主の正当性を示す署名データ $SIG_{M1, cp}$ を作成する。

そして、EMDサービスセンタ管理部125は、図18に示すように、コンテンツID、コンテンツ鍵データ K_c 、権利書データ106、電子透かし情報管理データWMおよびCP_IDと、これらについての署名データ $SIG_{M1, cp}$ とを格納した登録用モジュール Mod_2 を作成する。

【0164】

ステップA5：暗号化・復号部121は、ステップA4で作成した登録用モジュール Mod_2 を、ステップA2で共有したセッション鍵データ K_{SES} を用いて暗号化する。

ステップA6：EMDサービスセンタ管理部125は、ステップA5で暗号化した登録用モジュール Mod_2 をEMDサービスセンタ102に送信する。

【0165】

ステップA7以降の処理は、EMDサービスセンタ102における処理である。

ステップA7：EMDサービスセンタ102は、受信した登録用モジュール Mod_2 を、ステップA2において共有したセッション鍵データ K_{SES} を用いて復号する。

ステップA8：EMDサービスセンタ102は、復号した登録用モジュールM

o d₂に格納された署名データSIG_{M1, c p}を公開鍵データK_{CP, P}を用いて検証し、登録用モジュールMod₂の送り主の正当性を確認し、送り主の正当性が証明されたことを条件にステップA9の処理を行う。

ステップA9：EMDサービスセンタ102は、登録用モジュールMod₂に格納されているコンテンツID、コンテンツ鍵データK_c、権利書データ106、電子透かし情報管理データWMおよびCP_IDを所定のデータベースに格納して登録する。

【0166】

なお、EMDサービスセンタ管理部125は、図18に示すように、登録用モジュールMod₂に応じた登録処理がEMDサービスセンタ102に行われた後に、例えば6カ月分のキーファイルKFをEMDサービスセンタ102から受信し、相互認証部120とEMDサービスセンタ102との間の相互認証によって得たセッション鍵データK_{SES}を用いて、当該受信したキーファイルKFを復号した後にキーファイルデータベース118bに記憶する。

【0167】

次に、コンテンツプロバイダ101がユーザホームネットワーク103のSAM105₁にセキュアコンテナ104を送信する場合の処理を図3および図4を参照しながら説明する。

なお、以下の例では、コンテンツプロバイダ101からSAM105₁にセキュアコンテナ104を送信する場合を例示するが、セキュアコンテナ104をSAM105₂～105₄に送信する場合も、SAM105₁を介してSAM105₂～105₄に送信される点を除いて同じである。

まず、図3に示すように、コンテンツデータS111がコンテンツマスターデータベース111から読み出されて電子透かし情報付加部112に出力される。

次に、電子透かし情報付加部112は、コンテンツデータS111に電子透かし情報を埋め込んでコンテンツデータS112を生成し、これを圧縮部113に出力する。

次に、圧縮部113は、コンテンツデータS112を、例えばATRAC3方

式で圧縮してコンテンツデータ S 1 1 3 を作成し、これを暗号化部 1 1 4 に出力する。

また、図 4 に示すように、乱数発生部 1 1 5 において、乱数を発生してコンテンツ鍵データ K c が生成され、当該生成されたコンテンツ鍵データ K c が記憶部 1 1 9 に記憶される。

【0168】

次に、暗号化部 1 1 4 は、圧縮部 1 1 3 から入力したコンテンツデータ S 1 1 3 と、記憶部 1 1 9 から読み出したメタデータ M e t a、A/V 伸長用ソフトウェア S o f t および電子透かし情報管理データ W M とを、コンテンツ鍵データ K c を用いて暗号化してセキュアコンテナ作成部 1 1 8 に出力する。この場合に、メタデータ M e t a および電子透かし情報管理データ W M は暗号化しなくてもよい。

そして、セキュアコンテナ作成部 1 1 8 は、図 5 (A) に示すコンテンツファイル C F を作成する。また、署名処理部 1 1 7 において、コンテンツファイル C F のハッシュ値がとられ、秘密鍵データ K_{CP, S} を用いて署名データ S I G_{6, CP} が生成される。

【0169】

また、セキュアコンテナ作成部 1 1 8 は、キーファイルデータベース 1 1 8 b から、コンテンツデータ C に対応するキーファイル K F を読み出し、これを署名処理部 1 1 7 に出力する。

そして、署名処理部 1 1 7 は、セキュアコンテナ作成部 1 1 8 から入力したキーファイル K F のハッシュ値をとり、秘密鍵データ K_{CP, S} を用いて署名データ S I G_{7, CP} を生成し、これをセキュアコンテナ作成部 1 1 8 に出力する。

次に、セキュアコンテナ作成部 1 1 8 は、図 5 (A) に示すコンテンツファイル C F およびその署名データ S I G_{6, CP} と、図 5 (B) に示すキーファイル K F およびその署名データ S I G_{7, CP} と、記憶部 1 1 9 から読み出した図 5 (C) に示す公開鍵証明書データ C E R_{CP} およびその署名データ S I G_{1, ES} とを格納したセキュアコンテナ 1 0 4 を作成し、これを、セキュアコンテナデータベース 1 1 8 a に記憶する。そして、セキュアコンテナ作成部 1 1 8 は、

例えばユーザからの要求（リクエスト）に応じてユーザホームネットワーク 103 に提供しようとするセキュアコンテナ 104 をセキュアコンテナデータベース 118a から読み出して、相互認証部 120 と SAM 105₁ との間の相互認証によって得られたセッション鍵データ K_{SES} を用いて暗号化・復号部 121 において暗号化した後に、SAM 管理部 124 を介してユーザホームネットワーク 103 の SAM 105₁ に送信する。

【0170】

以下、コンテンツプロバイダ 101 の処理の全体の流れの概要を、セキュアコンテナ作成処理と関連付けて述べる。

図 20、図 21、図 22 は、当該処理の流れを説明するためのフローチャートである。

ステップ B1：コンテンツプロバイダ 101 は、予め自らの公開鍵証明書データ CER_{CP} を EMD サービスセンタ 102 から入力し、記憶部（データベース）119 に格納しておく。

ステップ B2：新しくオーサリングするコンテンツデータや、既に保管されているレガシーコンテンツデータなどのコンテンツマスターソースをデジタル化し、さらにコンテンツ ID を割り振り、コンテンツマスターソースデータベース 111 に格納して一元的に管理する。

ステップ B3：ステップ B1 において一元的に管理した各々のコンテンツマスターソースにメタデータ $Meta$ を作成し、これを記憶部 119 に格納する。

【0171】

ステップ B4：コンテンツマスターソースデータベース 111 からコンテンツマスターソースであるコンテンツデータ S111 を読み出して電子透かし情報付加部 112 に出力し、電子透かし情報を埋め込んでコンテンツデータ S112 を生成する。

ステップ B5：電子透かし情報付加部 112 は、埋め込みを行った電子透かし情報の内容と埋め込み位置とを所定のデータベースに格納する。

ステップ B6：圧縮部 113 において、電子透かし情報が埋め込まれたコンテンツデータ S112 を圧縮してコンテンツデータ S113 を生成する。

ステップB7：伸長部116
を伸長してコンテンツデータS

ステップB8：聴感検査部123に、
6の聴覚検査を行う。

ステップB9：コンテンツプロバイダ101は、
埋め込まれた電子透かし情報を、ステップB5でデータベ
タS113
タS11
6に
み内容および埋め込み位置に基づいて検出する。

そして、コンテンツプロバイダ101は、聴覚検査および電子透かし
出の双方が成功した場合には、ステップB10の処理を行い、何れか一方が失
した場合にはステップB4の処理を繰り返す。

【0172】

ステップB10：乱数発生部115において乱数してコンテンツ鍵データKc
を生成し、これを記憶部119に格納する。

ステップB11：暗号化部114において、圧縮したコンテンツデータS11
3を、コンテンツ鍵データKcを用いて暗号化してコンテンツデータCを作成す
る。

【0173】

ステップB12：権利書データ作成部122において、コンテンツデータCに
についての権利書データ106を作成する。

ステップB13：コンテンツプロバイダ101は、SRPを決定し、これを記
憶部119に格納する。

ステップB14：コンテンツプロバイダ101は、コンテンツID、コンテン
ツ鍵データKcおよび権利書データ106をEMDサービスセンタ102に出力
する。

ステップB15：コンテンツプロバイダ101は、配信用鍵データKD₁～K
D₃で暗号化されたキーファイルKFをEMDサービスセンタ102から入力す
る。

ステップB16：コンテンツプロバイダ101は、入力したキーファイルKF
をキーファイルデータベース118bに格納する。

コバイダ101は、コンテンツデータCとキーとハイパーリンクで結ぶ。

ステップA17において、コンテンツデータCおよびキーファイルについて、秘密鍵データ $K_{CP, S}$ を用いて、作成者の正当なを作成する。

ステップA19：セキュアコンテナ作成部118において、図5に示すセキュアコンテナ104を作成する。

【0175】

ステップB20：複数のセキュアコンテナを用いたコンポジット形式でコンテンツデータを提供する場合には、ステップB1～A19の処理を繰り返して各々のセキュアコンテナ104を作成し、コンテンツファイルCFとキーファイルKFとの間のリンク関係と、コンテンツファイルCF相互間のリンク関係とをハイパーリンクなどを用いて結ぶ。

ステップB21：コンテンツプロバイダ101は、作成したセキュアコンテナ104をセキュアコンテナデータベース118aに格納する。

【0176】

〔EMDサービスセンタ102〕

EMDサービスセンタ102は、認証(CA: Certificate Authority)機能、鍵管理(Key Management)機能および権利処理(Rights Clearing)(利益分配)機能を有する。

図23は、EMDサービスセンタ102の機能の構成図である。

図23に示すように、EMDサービスセンタ102は、鍵サーバ141、鍵データベース141a、決算処理部142、署名処理部143、決算機関管理部144、証明書・権利書管理部145、権利書データベース145a、証明書データベース145b、コンテンツプロバイダ管理部148、CPデータベース148a、SAM管理部149、SAMデータベース149a、相互認証部150、暗号化・復号部151およびKF作成部153を有する。

なお、図23には、EMDサービスセンタ102内の機能ブロック相互間のデ

ータの流れのうち、コンテンツプロバイダ 101 との間で送受信されるデータに関連するデータの流れが示されている。

また、図 24 には、EMD サービスセンタ 102 内の機能ブロック相互間のデータの流れのうち、SAM 105₁ ~ 105₄ および図 1 に示す決済機関 91 との間で送受信されるデータに関連するデータの流れが示されている。

【0177】

鍵サーバ 141 は、鍵データベース 141a に記憶された各々有効期間が 1 カ月の配信用鍵データを要求に応じて 6 か月分読み出して SAM 管理部 149 に出力する。

また、鍵データベース 141a 配信用鍵データ KD の他に、EMD サービスセンタ 102 の秘密鍵データ K_{ESC}, S、記録用鍵データ K_{STR}、メディア鍵データ K_{MED} および MAC 鍵データ K_{MAC} などの鍵データを記憶する一連の鍵データを格納している。

【0178】

決算処理部 142 は、SAM 105₁ ~ 105₄ から入力した利用履歴データ 108 と、証明書・権利書管理部 145 から入力した標準小売価格データ SRP および販売価格とに基づいて決済処理を行い、決済レポートデータ 107 および決済請求権データ 152 を作成し、決済レポートデータ 107 をコンテンツプロバイダ管理部 148 に出力し、決済請求権データ 152 を決算機関管理部 144 に出力する。

なお、決算処理部 142 は、販売価格に基づいて、違法なダンピング価格による取り引きが行われたか否かを監視する。

ここで、利用履歴データ 108 は、ユーザホームネットワーク 103 におけるセキュアコンテナ 104 の購入、利用（再生、記録および転送など）の履歴を示し、決算処理部 142 においてセキュアコンテナ 104 に関連したライセンス料の支払い額を決定する際に用いられる。

【0179】

利用履歴データ 108 には、例えば、セキュアコンテナ 104 に格納されたコンテンツデータ C の識別子であるコンテンツ ID、セキュアコンテナ 104 を配

給したコンテンツプロバイダ101の識別子CP_ID、セキュアコンテナ104内のコンテンツデータCの圧縮方法、セキュアコンテナ104を記録した記録媒体の識別子Media_ID、セキュアコンテナ104を配給を受けたSAM105₁～105₄の識別子SAM_ID、当該SAM105₁～105₄のユーザのUSER_IDなどが記述されている。従って、EMDサービスセンタ102は、コンテンツプロバイダ101の所有者以外にも、例えば、圧縮方法や記録媒体などのライセンス所有者に、ユーザホームネットワーク103のユーザが支払った金銭を分配する必要がある場合には、予め決められた分配率表に基づいて各相手に支払う金額を決定し、当該決定に応じた決済レポートデータ107および決済請求権データ152を作成する。当該分配率表は、例えば、セキュアコンテナ104に格納されたコンテンツデータ毎に作成される。

【0180】

また、決済請求権データ152は、当該データに基づいて、決済機関91に金銭の支払いを請求できる権威化されたデータであり、例えば、ユーザが支払った金銭を複数の権利者に配給する場合には、個々の権利者毎に作成される。

なお、決済機関91は、決済が終了すると、当該決済機関の利用明細書をEMDサービスセンタ102に送る。EMDサービスセンタ102は、当該利用明細書の内容を、対応する権利者に通知する。

【0181】

決算機関管理部144は、決算処理部142が生成した決済請求権データ152を図1に示すペイメントゲートウェイ90を介して決済機関91に送信する。

なお、後述するように、決算機関管理部144は、決済請求権データ152を、コンテンツプロバイダ101などの権利者に送信し、受信した決済請求権データ152を用いて、権利者自らが決済機関91に対しての決済を行ってもよい。

また、決算機関管理部144は、署名処理部143において決済請求権データ152のハッシュ値をとり、秘密鍵データK_{ESC}, Sを用いて生成した署名データSIG_gを決済請求権データ152と共に決済機関91に送信する。

【0182】

証明書・権利書管理部 145 は、証明書データベース 145b に登録（記録）されて権威化された公開鍵証明書データ CER_{CP} および公開鍵証明書データ $CER_{SAM1} \sim CER_{SAM4}$ などを読み出すと共に、コンテンツプロバイダ 101 の権利書データ 106、コンテンツ鍵データ Kc および電子透かし情報管理データ WM などを権利書データベース 145a に登録して権威化する。

ここで、権利書データベース 145a はコンテンツ ID を検索キーとして検索が行われ、証明書データベース 145b はコンテンツプロバイダ 101 の識別子 CP_ID を検索キーとして検索が行われる。

また、証明書・権利書管理部 145 は、例えば、権利書データ 106、コンテンツ鍵データ Kc および電子透かし情報管理データ WM などのハッシュ値をとり、秘密鍵データ $K_{ESC, S}$ を用いた署名データを付した権威化されたデータを権利書データベース 145a に格納する。

【0183】

コンテンツプロバイダ管理部 148 は、コンテンツプロバイダ 101 との間で通信する機能を有し、登録されたコンテンツプロバイダ 101 の識別子 CP_ID などを管理する CP データベース 148a にアクセスできる。

【0184】

SAM 管理部 149 は、ユーザホームネットワーク 103 内の $SAM105_1 \sim 105_4$ との間で通信する機能を有し、登録された SAM の識別子 SAM_ID や SAM 登録リストなどを記録した SAM データベース 149a にアクセスできる。

【0185】

KF 作成部 153 は、コンテンツプロバイダ管理部 148 から入力したコンテンツ鍵データ Kc および権利書データ 106 と、 SAM プログラム・ダウンロード・コンテナ $SDC_1 \sim SDC_3$ とを署名処理部 143 に出力する。

また、 KF 作成部 153 は、鍵サーバ 141 から入力した対応する期間の配信用鍵データ $KD_1 \sim KD_6$ を用いて、コンテンツ鍵データ Kc 、権利書データ 106 および SAM プログラム・ダウンロード・コンテナ $SDC_1 \sim SDC_3$ を暗号化し、図 5 (B) に示すように、当該暗号化したデータと、署名処理部 143

から入力した当該暗号化したデータについての秘密鍵データ $K_{ESC, S}$ による署名データ $SIG_{K1, ESC}$ とを格納したキーファイル KF を作成し、当該作成したキーファイル KF を KF データベース 153a に格納する。

【0186】

以下、EMDサービスセンタ 102 内での処理の流れを説明する。

まず、EMDサービスセンタ 102 からユーザホームネットワーク 103 内の $SAM105_1 \sim 105_4$ に配信用鍵データを送信する際の処理の流れを、図 24 を参照しながら説明する。

図 24 に示すように、鍵サーバ 141 は、所定期間毎に、例えば、3 カ月分の配信用鍵データ $KD_1 \sim KD_3$ を鍵データベース 141a から読み出して SAM 管理部 149 に出力する。

また、署名処理部 143 は、配信用鍵データ $KD_1 \sim KD_3$ の各々のハッシュ値をとり、EMDサービスセンタ 102 の秘密鍵データ $K_{ESC, S}$ を用いて、それぞれに対応する署名データ $SIG_{KD1, ESC} \sim SIG_{KD3, ESC}$ を作成し、これを SAM 管理部 149 に出力する。

SAM 管理部 149 は、この 3 カ月分の配信用鍵データ $KD_1 \sim KD_3$ およびそれらの署名データ $SIG_{KD1, ESC} \sim SIG_{KD3, ESC}$ を、相互認証部 150 と $SAM105_1 \sim 105_4$ と間の相互認証で得られたセッション鍵データ K_{SES} を用いて暗号化した後に、 $SAM105_1 \sim 105_4$ に送信する。

【0187】

次に、EMDサービスセンタ 102 がコンテンツプロバイダ 101 から、公開鍵証明書データ CER_{CP} の発行要求を受けた場合の処理を、図 23 を参照しながら説明する。

この場合に、コンテンツプロバイダ管理部 148 は、コンテンツプロバイダ 101 の識別子 CP_ID 、公開鍵データ $K_{CP, P}$ および署名データ SIG_9, CP をコンテンツプロバイダ 101 から受信すると、これらを、相互認証部 150 と図 4 に示す相互認証部 120 と間の相互認証で得られたセッション鍵データ K_{SES} を用いて復号する。

そして、当該復号した署名データ SIG_9, CP の正当性を署名処理部 143

において確認した後に、識別子 CP_ID および公開鍵データ $K_{CP, P}$ に基づいて、当該公開鍵証明書データの発行要求を出したコンテンツプロバイダ 101 が CP データベース 148a に登録されているか否かを確認する。

そして、証明書・権利書管理部 145 は、当該コンテンツプロバイダ 101 の公開鍵証明書データ CER_{CP} を証明書データベース 145b から読み出してコンテンツプロバイダ管理部 148 に出力する。

また、署名処理部 143 は、公開鍵証明書データ CER_{CP} のハッシュ値を取り、EMD サービスセンタ 102 の秘密鍵データ $K_{ESC, S}$ を用いて、署名データ SIG_1, ESC を作成し、これをコンテンツプロバイダ管理部 148 に出力する。

そして、コンテンツプロバイダ管理部 148 は、公開鍵証明書データ CER_{CP} およびその署名データ SIG_1, ESC を、相互認証部 150 と図 4 に示す相互認証部 120 と間の相互認証で得られたセッション鍵データ K_{SES} を用いて暗号化した後に、コンテンツプロバイダ 101 に送信する。

【0188】

次に、EMD サービスセンタ 102 が $SAM105_1$ から、公開鍵証明書データ CER_{SAM1} の発行要求を受けた場合の処理を、図 24 を参照しながら説明する。

この場合に、 SAM 管理部 149 は、 $SAM105_1$ の識別子 $SAM1_ID$ 、公開鍵データ $K_{SAM1, P}$ および署名データ $SIG_8, SAM1$ を $SAM105_1$ から受信すると、これらを、相互認証部 150 と $SAM105_1$ と間の相互認証で得られたセッション鍵データ K_{SES} を用いて復号する。

そして、当該復号した署名データ $SIG_8, SAM1$ の正当性を署名処理部 143 において確認した後に、識別子 $SAM1_ID$ および公開鍵データ $K_{SAM1, P}$ に基づいて、当該公開鍵証明書データの発行要求を出した $SAM105_1$ が SAM データベース 149a に登録されているか否かを確認する。

そして、証明書・権利書管理部 145 は、当該 $SAM105_1$ の公開鍵証明書データ CER_{SAM1} を証明書データベース 145b から読み出して SAM 管理部 149 に出力する。

また、署名処理部 143 は、公開鍵証明書データ CER_{SAM1} のハッシュ値をとり、EMD サービスセンタ 102 の秘密鍵データ $K_{ESC, S}$ を用いて、署名データ $SIG_{50, ESC}$ を作成し、これを SAM 管理部 149 に出力する。

そして、SAM 管理部 149 は、公開鍵証明書データ CER_{SAM1} およびその署名データ $SIG_{50, ESC}$ を、相互認証部 150 と $SAM105_1$ と間の相互認証で得られたセッション鍵データ K_{SES} を用いて暗号化した後に、 $SAM105_1$ に送信する。

なお、 $SAM105_2 \sim 105_4$ が、公開鍵証明書データを要求した場合の処理は、対象が $SAM105_2 \sim 105_4$ に代わるのみで、基本的に上述した $SAM105_1$ の場合と同じである。

なお、本発明では、EMD サービスセンタ 102 は、例えば、 $SAM105_1$ の出荷時に、 $SAM105_1$ の秘密鍵データ $K_{SAM1, S}$ および公開鍵データ $K_{SAM1, P}$ を $SAM105_1$ の記憶部に記憶する場合には、当該出荷時に、公開鍵データ $K_{SAM1, P}$ の公開鍵証明書データ CER_{SAM1} を作成してもよい。

このとき、当該出荷時に、公開鍵証明書データ CER_{SAM1} を、 $SAM105_1$ の記憶部に記憶してもよい。

【0189】

次に、EMD サービスセンタ 102 が、コンテンツプロバイダ 101 から図 18 に示す登録用モジュール Mod_2 を受けた場合の処理を、図 23 を参照しながら説明する。

この場合には、コンテンツプロバイダ管理部 148 がコンテンツプロバイダ 101 から図 18 に示す登録用モジュール Mod_2 を受信すると、相互認証部 150 と図 4 に示す相互認証部 120 と間の相互認証で得られたセッション鍵データ K_{SES} を用いて登録用モジュール Mod_2 を復号する。

そして、署名処理部 143 において、鍵データベース 141a から読み出した公開鍵データ $K_{cp, P}$ を用いて、署名データ $SIG_{M1, CP}$ の正当性を検証する。

次に、証明書・権利書管理部 145 は、登録用モジュール Mod_2 に格納され

た権利書データ106、コンテンツ鍵データKc、電子透かし情報管理データWMおよびSRPを、権利書データベース145aに登録する。

【0190】

次に、コンテンツプロバイダ管理部148は、コンテンツ鍵データKcおよび権利書データ106をKF作成部153に出力する。

次に、KF作成部153は、コンテンツプロバイダ管理部148から入力したコンテンツ鍵データKcおよび権利書データ106と、SAMプログラム・ダウンロード・コンテナSDC₁～SDC₃とを署名処理部143に出力する。

そして、署名処理部143は、KF作成部153から入力したデータ全体に対してハッシュ値をとり、EMDサービスセンタ102の秘密鍵データK_{ESC}, Sを用いて、その署名データSIG_{K1}, ESCを作成し、これをKF作成部153に出力する。

次に、KF作成部153において、鍵サーバ141から入力した対応する期間の配信用鍵データKD₁～KD₆を用いて、コンテンツ鍵データKcおよび権利書データ106と、SAMプログラム・ダウンロード・コンテナSDC₁～SDC₃を暗号化し、当該暗号化したデータと、署名処理部143から入力した署名データSIG_{K1}, ESCとを格納したキーファイルKFを作成し、これをKFデータベース153aに格納する。

ここで、SAMプログラム・ダウンロード・コンテナSDC₁～SDC₃は、登録用モジュールMod₂内に格納したものをを用いても、あるいはEMDサービスセンタ102が予め保持しているものをを用いてもよい。

次に、コンテンツプロバイダ管理部148は、KFデータベース153aにアクセスを行って得たキーファイルKFを、相互認証部150と図4に示す相互認証部120と間の相互認証で得られたセッション鍵データK_{SES}を用いて暗号化した後に、コンテンツプロバイダ101に送信する。

【0191】

次に、EMDサービスセンタ102において行なう決済処理を図24を参照しながら説明する。

SAM管理部149は、ユーザホームネットワーク103の例えばSAM10

5₁ から利用履歴データ 108 およびその署名データ SIG₂₀₀, SAM₁ を入力すると、利用履歴データ 108 および署名データ SIG₂₀₀, SAM₁ を、相互認証部 150 と SAM105₁ との間の相互認証によって得られたセッション鍵データ K_{SES} を用いて復号し、SAM105₁ の公開鍵データ K_{SAM₁} による署名データ SIG₂₀₀, SAM₁ の検証を行なった後に、決算処理部 142 に出力する。

【0192】

そして、決算処理部 142 は、SAM 管理部 149 から入力した利用履歴データ 108 と、証明書・権利書管理部 145 を介して権利書データベース 145a から読み出した権利書データ 106 に含まれる標準小売価格データ SRP および販売価格とに基づいて決済処理を行い、決済請求権データ 152 および決済レポートデータ 107 を生成する。

決算処理部 142 は、決済請求権データ 152 を決算機関管理部 144 に出力すると共に、決済レポートデータ 107 をコンテンツプロバイダ管理部 148 に出力する。

【0193】

次に、決算機関管理部 144 は、決済請求権データ 152 およびその署名データ SIG₉₉ を、相互認証およびセッション鍵データ K_{SES} による復号を行なった後に、図 1 に示すペイメントゲートウェイ 90 を介して決済機関 91 に送信する。

これにより、決済請求権データ 152 に示される金額の金銭が、コンテンツプロバイダ 101 に支払われる。

【0194】

次に、EMD サービスセンタ 102 がコンテンツプロバイダ 101 に決済レポートを送信する場合の処理を図 23 を参照しながら説明する。

決算処理部 142 において決済が行なわれると、前述したように、決算処理部 142 からコンテンツプロバイダ管理部 148 に決済レポートデータ 107 が出力される。

決済レポートデータ 107 は、上述したように、例えば、EMD サービスセン

タ 102 が図 1 に示す決済機関 91 に対して行なったコンテンツプロバイダ 101 に関する決済の内容が記述されている。

EMD サービスセンタ 102 は、決算処理部 142 から決済レポートデータ 107 を入力すると、これを、相互認証部 150 と図 4 に示す相互認証部 120 と間の相互認証で得られたセッション鍵データ K_{SES} を用いて暗号化した後に、コンテンツプロバイダ 101 に送信する。

【0195】

また、EMD サービスセンタ 102 は、前述したように、権利書データ 106 を登録（権威化）した後に、EMD サービスセンタ 102 からコンテンツプロバイダ 101 に、権威化証明書モジュールを配信用鍵データ $KD_1 \sim KD_6$ で暗号化して送信してもよい。

【0196】

また、EMD サービスセンタ 102 は、その他に、 $SAM105_1 \sim 105_4$ の出荷時の処理と、SAM 登録リストの登録処理とを行なうが、これらの処理については後述する。

【0197】

〔ユーザホームネットワーク 103〕

ユーザホームネットワーク 103 は、図 1 に示すように、ネットワーク機器 160₁ および A/V 機器 160₂ ~ 160₄ を有している。

ネットワーク機器 160₁ は、 $SAM105_1$ を内蔵している。また、A/V 機器 160₂ ~ 160₄ は、それぞれ $SAM105_2 \sim 105_4$ を内蔵している。

$SAM105_1 \sim 105_4$ の相互間は、例えば、IEEE 1394 シリアルインタフェースバスなどのバス 191 を介して接続されている。

なお、A/V 機器 160₂ ~ 160₄ は、ネットワーク通信機能を有していてもよいし、ネットワーク通信機能を有しておらず、バス 191 を介してネットワーク機器 160₁ のネットワーク通信機能を利用してもよい。

また、ユーザホームネットワーク 103 は、ネットワーク機能を有していない A/V 機器のみを有していてもよい。

【0198】

以下、ネットワーク機器 160₁ について説明する。

図 25 は、ネットワーク機器 160₁ の構成図である。

図 25 に示すように、ネットワーク機器 160₁ は、SAM105₁、通信モジュール 162、復号・伸長モジュール 163、購入・利用形態決定操作部 165、ダウンロードメモリ 167、再生モジュール 169 および外部メモリ 201 を有する。

【0199】

SAM105₁ ~ 105₄ は、コンテンツ単位の課金処理をおこなうモジュールであり、EMD サービスセンタ 102 との間で通信を行う。

SAM105₁ ~ 105₄ は、例えば、EMD サービスセンタ 102 によって仕様およびバージョンなどが管理され、家庭機器メーカーに対し、搭載の希望があればコンテンツ単位の課金を行うブラックボックスの課金モジュールとしてライセンス譲渡される。例えば、家庭機器開発メーカーは、SAM105₁ ~ 105₄ の IC (Integrated Circuit) の内部の仕様を知ることではできず、EMD サービスセンタ 102 が当該 IC のインタフェースなどを統一化し、それによってネットワーク機器 160₁ および AV 機器 160₂ ~ 160₄ に搭載される。

【0200】

SAM105₁ ~ 105₄ は、その処理内容が外部から完全に遮蔽され、その処理内容を外部から監視および改竄不能であり、また、内部に予め記憶されているデータおよび処理中のデータを外部から監視および改竄不能な耐タンパ (Tamper Resistance) 性を持ったハードウェアモジュール (IC モジュールなど) である。

SAM105₁ ~ 105₄ の機能を IC という形で実現する場合は、IC 内部に秘密メモリを持ち、そこに秘密プログラムおよび秘密データが格納される。SAM を IC という物理的形態にとらわれず、その機能を機器の何れかの部分に組み込むことができれば、その部分を SAM として定義してもよい。

【0201】

以下、SAM105₁ の機能について詳細に説明する。

なお、SAM105₂～105₄は、SAM105₁と基本的に同じ機能を有している。

図26は、SAM105₁の機能の構成図である。

なお、図26には、コンテンツプロバイダ101からのセキュアコンテナ104を入力し、セキュアコンテナ104内のキーファイルKFを復号する処理に関連するデータの流れが示されている。

図26に示すように、SAM105₁は、相互認証部170、暗号化・復号部171、172、173、コンテンツプロバイダ管理部180、誤り訂正部181、ダウンロードメモリ管理部182、セキュアコンテナ復号部183、復号・伸長モジュール管理部184、EMDサービスセンタ管理部185、利用監視部186、課金処理部187、署名処理部189、SAM管理部190、メディアSAM管理部197、スタック（作業）メモリ200および外部メモリ管理部811を有する。

なお、AV機器160₂～160₄はダウンロードメモリ167を有していないため、SAM105₂～105₄にはダウンロードメモリ管理部182は存在しない。

【0202】

なお、図26に示すSAM105₁の所定の機能は、例えば、図示しないCPUにおいて秘密プログラムを実行することによって実現される。

また、外部メモリ201には、以下に示す処理を経て、図27に示すように、利用履歴データ108およびSAM登録リストが記憶される。

ここで、外部メモリ201のメモリ空間は、SAM105₁の外部（例えば、ホストCPU810）からは見ることはできず、SAM105₁のみが外部メモリ201の記憶領域に対してのアクセスを管理できる。

外部メモリ201としては、例えば、フラッシュメモリあるいは強誘電体メモリ（FeRAM）などが用いられる。

また、スタックメモリ200としては、例えばSARAMが用いられ、図28に示すように、セキュアコンテナ104、コンテンツ鍵データK_c、権利書データ（UCP）106、記憶部192のロック鍵データK_{LOC}、コンテンツプロ

バイダ101の公開鍵証明書 CER_{CP} 、利用制御状態データ(UCS)166、およびSAMプログラム・ダウンロード・コンテナ $SDC_1 \sim SDC_3$ などが記憶される。

【0203】

以下、 $SAM105_1$ の機能のうち、コンテンツプロバイダ101からのセキュアコンテナ104を入力したときの各機能ブロックの処理内容を図26を参照しながら説明する。

【0204】

相互認証部170は、 $SAM105_1$ がコンテンツプロバイダ101およびEMDサービスセンタ102との間でオンラインでデータを送受信する際に、コンテンツプロバイダ101およびEMDサービスセンタ102との間で相互認証を行ってセッション鍵データ(共有鍵) K_{SES} を生成し、これを暗号化・復号部171に出力する。セッション鍵データ K_{SES} は、相互認証を行う度に新たに生成される。

【0205】

暗号化・復号部171は、コンテンツプロバイダ101およびEMDサービスセンタ102との間で送受信するデータを、相互認証部170が生成したセッション鍵データ K_{SES} を用いて暗号化・復号する。

【0206】

誤り訂正部181は、セキュアコンテナ104を誤り訂正してダウンロードメモリ管理部182に出力する。

なお、ユーザホームネットワーク103は、セキュアコンテナ104が改竄されているか否かを検出する機能を有していてもよい。

本実施形態では、誤り訂正部181を、 $SAM105_1$ に内蔵した場合を例示したが、誤り訂正部181の機能を、例えばホストCPU810などの $SAM105_1$ の外部に持たせてもよい。

【0207】

ダウンロードメモリ管理部182は、図25に示すようにダウンロードメモリ167が相互認証機能を持つメディア $SAM167a$ を有している場合には、相

互認証部 170 とメディア SAM 167 a との間で相互認証を行った後に、誤り訂正後のセキュアコンテナ 104 を、相互認証によって得られたセッション鍵データ K_{SES} を用いて暗号化して図 25 に示すダウンロードメモリ 167 に書き込む。ダウンロードメモリ 167 としては、例えば、メモリスティックなどの不揮発性半導体メモリが用いられる。

なお、図 29 に示すように、HDD (Hard Disk Drive) などの相互認証機能を備えていないメモリをダウンロードメモリ 211 として用いる場合には、ダウンロードメモリ 211 内はセキュアではないので、コンテンツファイル CF をダウンロードメモリ 211 にダウンロードし、機密性の高いキーファイル KF を例えば、図 26 に示すスタックメモリ 200 にダウンロードする。

【0208】

セキュアコンテナ復号部 183 は、ダウンロードメモリ管理部 182 から入力したセキュアコンテナ 104 に格納されたキーファイル KF 内のコンテンツ鍵データ K_c 、権利書データ 106 および SAM プログラム・ダウンロード・コンテナ $SDC_1 \sim SDC_3$ を、記憶部 192 から読み出した対応する期間の配信用鍵データ $KD_1 \sim KD_3$ を用いて復号する。

当該復号されたコンテンツ鍵データ K_c 、権利書データ 106 および SAM プログラム・ダウンロード・コンテナ $SDC_1 \sim SDC_3$ は、スタックメモリ 200 に書き込まれる。

【0209】

EMD サービスセンタ管理部 185 は、図 1 に示す EMD サービスセンタ 102 との間の通信を管理する。

【0210】

署名処理部 189 は、記憶部 192 から読み出した EMD サービスセンタ 102 の公開鍵データ $K_{ESC, P}$ およびコンテンツプロバイダ 101 の公開鍵データ $K_{CP, P}$ を用いて、セキュアコンテナ 104 内の署名データの検証を行なう。

【0211】

記憶部 192 は、SAM 105₁ の外部から読み出しおよび書き換えできない

秘密データとして、図30に示すように、有効期限付きの複数の配信用鍵データ $KD_1 \sim KD_3$ 、 SAM_ID 、ユーザID、パスワード、情報参照用ID、 SAM 登録リスト、記録用鍵データ K_{STR} 、ルートCAの公開鍵データ $K_{R-C_A, P}$ 、EMDサービスセンタ102の公開鍵データ $K_{ESC, P}$ 、メディア鍵データ K_{MED} 、EMDサービスセンタ102の公開鍵データ $K_{ESC, P}$ 、 $SAM105_1$ の秘密鍵データ $K_{SAM1, S}$ 、 $SAM105_1$ の公開鍵データ $K_{SAM1, P}$ を格納した公開鍵証明書 CER_{SAM1} 、EMDサービスセンタ102の秘密鍵データ $K_{ESC, S}$ を用いた公開鍵証明書 CER_{ESC} の署名データ SIG_{22} 、復号・伸長モジュール163との間の相互認証用の元鍵データ（共通鍵暗号化方式を採用した場合）、メディアSAMとの間の相互認証用の元鍵データ（共通鍵暗号化方式を採用した場合）、並びにメディアSAMの公開鍵証明書データ CER_{MEDSAM} （公開鍵暗号化方式を採用した場合）を記憶している。

また、記憶部192には、図26に示す少なくとも一部の機能を実現するための秘密プログラムが記憶されている。

記憶部192としては、例えば、フラッシュ-EEPROM (Electrically Erasable Programmable RAM) が用いられる。

【0212】

以下、EMDサービスセンタ102から受信した配信用鍵データ $KD_1 \sim KD_3$ を記憶部192に格納する際の $SAM105_1$ 内での処理の流れを図26を参照しながら説明する。

この場合には、まず、相互認証部170と図23に示す相互認証部150との間で相互認証が行われる。

次に、当該相互認証によって得られたセッション鍵データ K_{SES} で暗号化された3カ月分の配信用鍵データ $KD_1 \sim KD_3$ およびその署名データ $SIG_{KD1, ESC} \sim SIG_{KD3, ESC}$ が、EMDサービスセンタ102からEMDサービスセンタ管理部185を介してスタックメモリ811に書き込まれる。

次に、暗号化・復号部171において、セッション鍵データ K_{SES} を用いて

、配信用鍵データ $KD_1 \sim KD_3$ およびその署名データ $SIG_{KD1, ESC} \sim SIG_{KD3, ESC}$ が復号される。

次に、署名処理部 189 において、スタックメモリ 811 に記憶された署名データ $SIG_{KD1, ESC} \sim SIG_{KD3, ESC}$ の正当性が確認された後に、配信用鍵データ $KD_1 \sim KD_3$ が記憶部 192 に書き込まれる。

【0213】

以下、コンテンツプロバイダ 101 が提供したセキュアコンテナ 104 を入力する際の SAM_{105_1} 内での処理の流れを図 26 を参照しながら説明する。

図 26 に示す SAM_{105_1} の相互認証部 170 と図 3 に示す相互認証部 120 との間で相互認証が行なわれる。

暗号化・復号部 171 は、当該相互認証によって得られたセッション鍵データ K_{SES} を用いて、コンテンツプロバイダ管理部 180 を介してコンテンツプロバイダ 101 から供給されたセキュアコンテナ 104 を復号する。

【0214】

次に、署名処理部 189 は、図 5 (C) に示す署名データ $SIG_{1, ESC}$ の検証を行なった後に、図 5 (C) に示す公開鍵証明書データ CER_{CP} 内に格納されたコンテンツプロバイダ 101 の公開鍵データ $K_{CP, P}$ を用いて、署名データ $SIG_{6, CP}, SIG_{7, CP}$ の正当性を検証する。

このとき、署名データ $SIG_{6, CP}$ が正当であると検証されたときに、コンテンツファイル CF の作成者および送信者の正当性が確認される。

また、署名データ $STG_{7, CP}$ が正当であると検証されたときに、キーファイル KF の送信者の正当性が確認される。

また、署名処理部 189 は、記憶部 192 から読み出した公開鍵データ $K_{ESC, P}$ を用いて、図 5 (B) に示すキーファイル KF 内の署名データ $SIG_{K1, ESC}$ の正当性、すなわちキーファイル KF の作成者の正当性およびキーファイル KF が EMD サービスセンタ 102 に登録されているか否かの検証を行う。

コンテンツプロバイダ管理部 180 は、署名データ $SIG_{6, CP}, SIG_{7, CP}, SIG_{K1, ESC}$ の正当性が確認されると、セキュアコンテナ 104 を誤り訂正部 181 に出力する。

【0215】

誤り訂正部181は、セキュアコンテナ104を誤り訂正した後に、ダウンロードメモリ管理部182に出力する。

ダウンロードメモリ管理部182は、相互認証部170と図25に示すメディアSAM167aとの間で相互認証を行なった後に、セキュアコンテナ104をダウンロードメモリ167に書き込む。

【0216】

次に、ダウンロードメモリ管理部182は、相互認証部170と図25に示すメディアSAM167aとの間で相互認証を行なった後に、セキュアコンテナ104に格納された図5(B)に示すキーファイルKFをダウンロードメモリ167から読み出してセキュアコンテナ復号部183に出力する。

【0217】

そして、セキュアコンテナ復号部183において、記憶部192から入力した対応する期間の配信用鍵データ $KD_1 \sim KD_3$ を用いて、図5(B)に示すキーファイルKF内のコンテンツ鍵データKc、権利書データ106およびSAMプログラム・ダウンロード・コンテナ $SDC_1 \sim SDC_3$ が復号される。

そして、復号されたコンテンツ鍵データKc、権利書データ106およびSAMプログラム・ダウンロード・コンテナ $SDC_1 \sim SDC_3$ がスタックメモリ200に書き込まれる。

【0218】

以下、ダウンロードメモリ167にダウンロードされたコンテンツデータCを利用・購入する処理に関連する各機能ブロックの処理内容を図31を参照しながら説明する。

【0219】

利用監視部186は、スタックメモリ200から権利書データ106および利用制御状態データ166を読み出し、当該読み出した権利書データ106および利用制御状態データ166によって許諾された範囲内でコンテンツの購入・利用が行われるように監視する。

ここで、権利書データ106は、図26を用いて説明したように、復号後にK

Fに格納されてスタックメモリ200に記憶されている。

また、利用制御状態データ166は、後述するように、ユーザによって購入形態が決定されたときに、スタックメモリ200に記憶される。

【0220】

課金処理部187は、図25に示す購入・利用形態決定操作部165からの操作信号S165に応じた利用履歴データ108を作成する。

ここで、利用履歴データ108は、前述したように、ユーザによるセキュアコンテナ104の購入および利用の形態の履歴を記述しており、EMDサービスセンタ102において、セキュアコンテナ104の購入に応じた決済処理およびライセンス料の支払いを決定する際に用いられる。

【0221】

また、課金処理部187は、必要に応じて、スタックメモリ200から読み出した販売価格あるいは標準小売価格データSRPをユーザに通知する。

ここで、販売価格および標準小売価格データSRPは、復号後にスタックメモリ200に記憶された図5(B)に示すキーファイルKFの権利書データ106内に格納されている。

課金処理部187による課金処理は、利用監視部186の監視の下、権利書データ106が示す使用許諾条件などの権利内容および利用制御状態データ166に基づいて行われる。すなわち、ユーザは、当該権利内容などに従った範囲内でコンテンツの購入および利用を行う。

【0222】

また、課金処理部187は、操作信号S165に基づいて、ユーザによって決定されたコンテンツの購入形態を記述した利用制御状態(UCS: Usage Control Status)データ166を生成し、これをスタックメモリ200に書き込む。

コンテンツの購入形態としては、例えば、購入者による再生や当該購入者の利用のための複製に制限を加えない買い切りや、再生する度に課金を行なう再生課金などがある。

ここで、利用制御状態データ166は、ユーザがコンテンツの購入形態を決定

したときに生成され、以後、当該決定された購入形態で許諾された範囲内でユーザが当該コンテンツの利用を行なうように制御するために用いられる。利用制御状態データ166には、コンテンツのID、購入形態、当該購入形態に応じた価格、当該コンテンツの購入が行なわれたSAMのSAM_ID、購入を行なったユーザのUSER_IDなどが記述されている。

【0223】

なお、決定された購入形態が再生課金である場合には、例えば、SAM105₁からコンテンツプロバイダ101に利用制御状態データ166をコンテンツデータCの購入と同時にリアルタイムに送信し、コンテンツプロバイダ101がEMDサービスセンタ102に、利用履歴データ108を所定の期間内にSAM105₁に取りにいくことを指示する。

また、決定された購入形態が買い切りである場合には、例えば、利用制御状態データ166が、コンテンツプロバイダ101およびEMDサービスセンタ102の双方にリアルタイムに送信される。このように、本実施形態では、何れの場合にも、利用制御状態データ166をコンテンツプロバイダ101にリアルタイムに送信する。

【0224】

EMDサービスセンタ管理部185は、外部メモリ管理部811を介して外部メモリ201から読み出した利用履歴データ108をEMDサービスセンタ102に送信する。

このとき、EMDサービスセンタ管理部185は、署名処理部189において、秘密鍵データ $K_{SAM1, s}$ を用いて利用履歴データ108の署名データSIG_{200, SAM1}を作成し、署名データSIG_{200, SAM1}を利用履歴データ108と共にEMDサービスセンタ102に送信する。

EMDサービスセンタ102への利用履歴データ108の送信は、例えば、EMDサービスセンタ102からの要求に応じてあるいは定期的に行ってもよいし、利用履歴データ108に含まれる履歴情報の情報量が所定以上になったときに行ってもよい。当該情報量は、例えば、外部メモリ201の記憶容量に応じて決定される。

【0225】

ダウンロードメモリ管理部182は、例えば、図25に示す購入形態決定操作部165からの操作信号S165に応じてコンテンツの再生動作が行われる場合に、ダウンロードメモリ167から読み出したコンテンツデータC、スタックメモリ200から読み出したコンテンツ鍵データKcおよび課金処理部187から入力したユーザ電子透かし情報用データ196を復号・伸長モジュール管理部184に出力する。

また、復号・伸長モジュール管理部184は、図25に示す購入形態決定操作部165からの操作信号S165に応じてコンテンツの試聴動作が行われる場合に、ダウンロードメモリ167から読み出したコンテンツファイルCF、並びにスタックメモリ200から読み出したコンテンツ鍵データKcおよび半開示パラメータデータ199を復号・伸長モジュール管理部184に出力する。

【0226】

ここで、半開示パラメータデータ199は、権利書データ106内に記述されており、試聴モード時のコンテンツの取り扱いを示している。復号・伸長モジュール163では、半開示パラメータデータ199に基づいて、暗号化されたコンテンツデータCを、半開示状態で再生することが可能になる。半開示の手法としては、例えば、復号・伸長モジュール163がデータ（信号）を所定のブロックを単位として処理することを利用して、半開示パラメータデータ199によって、コンテンツ鍵データKcを用いて復号を行うブロックと復号を行わないブロックとを指定したり、試聴時の再生機能を限定したり、試聴可能な期間を限定するものなどがある。

【0227】

以下、SAM105₁内での処理の流れについて説明する。

まず、コンテンツプロバイダ101からダウンロードメモリ167にダウンロードされたセキュアコンテナ104の購入形態を決定するまでの処理の流れを図31を参照しながら説明する。

ユーザによる図25に示す購入・利用形態決定操作部165の操作によって、試聴モードを示す操作信号S165が課金処理部187に出力されると、例えば

、ダウンロードメモリ 167 に記憶されているコンテンツファイル CF が、復号・伸長モジュール管理部 184 を介して、図 25 に示す復号・伸長モジュール 163 に出力される。

このとき、コンテンツファイル CF に対して、相互認証部 170 とメディア SAM 167a との間の相互認証およびセッション鍵データ K_{SES} による暗号化・復号と、相互認証部 170 と相互認証部 220 との間の相互認証およびセッション鍵データ K_{SES} による暗号化・復号とが行なわれる。

コンテンツファイル CF は、図 25 に示す復号部 221 においてセッション鍵データ K_{SES} を用いて復号された後に、復号部 222 に出力される。

【0228】

また、スタックメモリ 200 から読み出されたコンテンツ鍵データ K_c および半開示パラメータデータ 199 が、図 25 に示す復号・伸長モジュール 163 に出力される。このとき、相互認証部 170 と相互認証部 220 との間の相互認証後に、コンテンツ鍵データ K_c および半開示パラメータデータ 199 に対してセッション鍵データ K_{SES} による暗号化および復号が行なわれる。

次に、復号された半開示パラメータデータ 199 が半開示処理部 225 に出力され、半開示処理部 225 からの制御によって、復号部 222 によるコンテンツ鍵データ K_c を用いたコンテンツデータ C の復号が半開示で行われる。

次に、半開示で復号されたコンテンツデータ C が、伸長部 223 において伸長された後に、電子透かし情報処理部 224 に出力される。

次に、電子透かし情報処理部 224 においてユーザ電子透かし情報用データ 196 がコンテンツデータ C に埋め込まれた後、コンテンツデータ C が再生モジュール 169 において再生され、コンテンツデータ C に応じた音響が出力される。

【0229】

そして、コンテンツを試聴したユーザが、購入・利用形態決定操作部 165 を操作して購入形態を決定すると、当該決定した購入形態を示す操作信号 S165 が課金処理部 187 に出力される。

そして、課金処理部 187 において、決定された購入形態に応じた利用履歴データ 108 および利用制御状態データ 166 が生成され、利用履歴データ 108

が外部メモリ管理部 811 を介して外部メモリ 201 に書き込まれると共に、利用制御状態データ 166 がスタックメモリ 200 に書き込まれる。

以後は、利用監視部 186 において、利用制御状態データ 166 によって許諾された範囲で、コンテンツの購入および利用が行なわれるように制御（監視）される。

【0230】

そして、後述する図 34 (C) に示す新たなキーファイル KF_1 が作成され、当該作成されたキーファイル KF_1 がダウンロードメモリ管理部 182 を介してダウンロードメモリ 167 に記憶される。

図 34 (C) に示すように、キーファイル KF_1 に格納された利用制御状態データ 166 はストレージ鍵データ K_{STR} およびメディア鍵データ K_{MED} を用いて DES の CBC モードを利用して順に暗号化されている。

ここで、記録用鍵データ K_{STR} は、例えば SACD (Super Audio Compact Disc)、DVD (Digital Versatile Disc) 機器、CD-R 機器および MD (Mini Disc) 機器などの種類に応じて決まるデータであり、機器の種類と記録媒体の種類とを 1 対 1 で対応づけるために用いられる。また、メディア鍵データ K_{MED} は、記録媒体にユニークなデータである。

【0231】

また、署名処理部 189 において、 $SAM105_1$ の秘密鍵データ K_{SAM1} 、 S を用いて、キーファイル KF_1 のハッシュ値 H_{K1} が作成され、当該作成されたハッシュ値 H_{K1} が、キーファイル KF_1 と対応付けられてスタックメモリ 200 に書き込まれる。ハッシュ値 H_{K1} は、キーファイル KF_1 の作成者の正当性およびキーファイル KF_1 が改竄されたか否かを検証するために用いられる。

【0232】

次に、ダウンロードメモリ 167 に記憶されている購入形態が既に決定されたコンテンツデータ C を再生する場合の処理の流れを、図 31 を参照しながら説明する。

この場合には、利用監視部 186 の監視下で、操作信号 S165 に基づいて、ダウンロードメモリ 167 に記憶されているコンテンツファイル CF が、図 31 に示す復号・伸長モジュール 163 に出力される。このとき、図 31 に示す相互認証部 170 と、図 25 に示す復号・伸長モジュール 163 の相互認証部 220 との間で相互認証が行われる。

また、スタックメモリ 200 から読み出されたコンテンツ鍵データ Kc が復号・伸長モジュール 163 に出力される。

そして、復号・伸長モジュール 163 の復号部 222 において、コンテンツ鍵データ Kc を用いたコンテンツファイル CF の復号と、伸長部 223 による伸長処理とが行なわれ、再生モジュール 169 において、コンテンツデータ C が再生される。

このとき、課金処理部 187 によって、操作信号 S165 に応じて、外部メモリ 201 に記憶されている利用履歴データ 108 が更新される。

利用履歴データ 108 は、外部メモリ 201 から読み出された後、相互認証を経て、EMD サービスセンタ管理部 185 を介して、署名データ SIG₂₀₀、SAM₁ と共に EMD サービスセンタ 102 に送信される。

【0233】

次に、図 32 に示すように、例えば、前述したようにネットワーク機器 160₁ のダウンロードメモリ 167 にダウンロードされたコンテンツファイル CF の購入形態を決定した後に、当該コンテンツファイル CF を格納した新たなセキュアコンテナ 104x を生成し、バス 191 を介して、AV 機器 160₂ の SAM 105₂ にセキュアコンテナ 104x を転送する場合の SAM 105₁ 内での処理の流れを図 33 を参照しながら説明する。

ユーザは、購入・利用形態決定操作部 165 を操作して、ダウンロードメモリ 167 に記憶された所定のコンテンツを AV 機器 160₂ に転送することを指示し、当該操作に応じた操作信号 S165 が、課金処理部 187 に出力される。

これにより、課金処理部 187 は、操作信号 S165 に基づいて、外部メモリ 201 に記憶されている利用履歴データ 108 を更新する。

また、課金処理部 187 は、コンテンツデータの購入形態が決定される度に、

当該決定された購入形態を示す利用制御状態データ166をEMDサービスセンタ管理部185を介してEMDサービスセンタ102に送信する。

【0234】

また、ダウンロードメモリ管理部182は、ダウンロードメモリ167から読み出した図5(A)に示すコンテンツファイルCFおよびその署名データSIG₆, CPと、キーファイルKFおよびその署名データSIG₇, CPと、キーファイルKF₁およびそのハッシュ値H_{K1}とをSAM管理部190に出力する。このとき、SAM105₁の相互認証部170とメディアSAM167aとの間の相互認証およびセッション鍵データK_{SES}による暗号化・復号が行われる。

また、署名処理部189は、コンテンツファイルCFのハッシュ値をとり、秘密鍵データK_{SAM1, S}を用いて署名データSIG₄₁, SAM₁を作成し、これをSAM管理部190に出力する。

また、署名処理部189は、キーファイルKF₁のハッシュ値をとり、秘密鍵データK_{SAM1, S}を用いて署名データSIG₄₂, SAM₁を作成し、これをSAM管理部190に出力する。

また、SAM管理部190は、記憶部192から、図34(D)に示す公開鍵証明書データCER_{CP}およびその署名データSIG_{1, ESC}と、公開鍵証明書データCER_{SAM1}およびその署名データSIG_{22, ESC}を読み出す。

【0235】

また、相互認証部170は、SAM105₂との間で相互認証を行って得たセッション鍵データK_{SES}を暗号化・復号部171に出力する。

SAM管理部190は、図34(A), (B), (C), (D)に示すデータからなる新たなセキュアコンテナ104xを生成し、暗号化・復号部171において、セッション鍵データK_{SES}を用いてセキュアコンテナ104xを暗号化した後に、図32に示すAV機器160₂のSAM105₂に出力する。

このとき、SAM105₁とSAM105₂との間の相互認証と並行して、IEEE1394シリアルバスであるバス191の相互認証が行われる。

【0236】

以下、図32に示すように、SAM105₁から入力したセキュアコンテナ104xを、RAM型などの記録媒体（メディア）130₄に書き込む際のSAM105₂内での処理の流れを、図35を参照しながら説明する。

ここで、RAM型の記録媒体130₄は、例えば、セキュアでないRAM領域134、メディアSAM133およびセキュアRAM領域132を有している。

【0237】

この場合には、SAM105₂のSAM管理部190は、図32および図35に示すように、ネットワーク機器160₁のSAM105₁からセキュアコンテナ104xを入力する。

そして、暗号化・復号部171において、SAM管理部190を介して入力したセキュアコンテナ104xが、相互認証部170とSAM105₁の相互認証部170との間の相互認証によって得られたセッション鍵データK_{SES}を用いて復号される。

【0238】

次に、署名処理部189において、公開鍵データK_{CP, P}を用いて、署名データSIG_{6, CP}の正当性が検証され、コンテンツファイルCFの作成者の正当性が確認される。また、署名処理部189において、公開鍵データK_{SAM1, P}を用いて、署名データSIG_{41, SAM1}の正当性が検証され、コンテンツファイルCFの送信者の正当性が確認される。

そして、コンテンツファイルCFの作成者および送信者が正当であると確認された後に、SAM管理部190から記録モジュール管理部855にコンテンツファイルCFが出力され、コンテンツファイルCFが図32に示すRAM型の記録媒体130₄のRAM領域134に書き込まれる。

【0239】

また、セッション鍵データK_{SES}を用いて復号されたキーファイルKFおよびその署名データSIG_{7, CP}、SIG_{42, SAM1}と、キーファイルKF₁およびそのハッシュ値H_{K1}と、公開鍵署名データCER_{CP}およびその署名データSIG_{1, ESC}と、公開鍵署名データCER_{SAM1}およびその署名データSIG_{22, ESC}とが、スタックメモリ200に書き込まれる。

【0240】

次に、署名処理部189は、スタックメモリ200から読み出した署名データSIG₂₂, ESCを、記憶部192から読み出した公開鍵データK_{ESC, P}を用いて検証して、公開鍵証明書データCER_{SAM1}の正当性を確認する。

そして、署名処理部189は、公開鍵証明書データCER_{SAM1}の正当性を確認すると、公開鍵証明書データCER_{SAM1}に格納された公開鍵データK_{SAM1, P}を用いて、スタックメモリ200に記憶されている署名データSIG₄₂, SAM₁の正当性を検証する。そして、署名データSIG₄₂, SAM₁が正当であると検証されたときに、キーファイルKFの送信者の正当性が確認される。

また、署名処理部189は、スタックメモリ200から読み出した署名データSIG₁, ESCを、記憶部192から読み出した公開鍵データK_{ESC, P}を用いて検証して、公開鍵証明書データCER_{CP}の正当性を確認する。

そして、署名処理部189は、公開鍵証明書データCER_{CP}の正当性を確認すると、公開鍵証明書データCER_{CP}に格納された公開鍵データK_{CP, P}を用いて、スタックメモリ200に記憶されている署名データSIG₇, SAM₁の正当性を検証する。そして、署名データSIG₇, SAM₁が正当であると検証されたときに、キーファイルKFの作成者の正当性が確認される。

キーファイルKFの作成者および送信者が正当であることが確認されると、キーファイルKFがスタックメモリ200から読み出され、記録モジュール管理部855を介して、図34に示すRAM型の記録媒体130₄のセキュアRAM領域132に書き込まれる。

【0241】

また、署名処理部189は、公開鍵データK_{SAM1, P}を用いて、ハッシュ値H_{K1}の正当性を検証し、キーファイルKF₁の作成者および送信者の正当性を確認する。

そして、キーファイルKF₁の作成者および送信者の正当性が確認されると、図34(C)に示すキーファイルKF₁をスタックメモリ200から読み出して暗号化・復号部173に出力する。

なお、当該例では、キーファイル KF_1 の作成者と送信元とが同じ場合を述べたが、キーファイル KF_1 の作成者と送信元とが異なる場合には、キーファイル KF_1 に対して作成者の署名データと送信者と署名データとが作成され、署名処理部189において、双方の署名データの正当性が検証される。

【0242】

そして、暗号化・復号部173は、記憶部192から読み出した記録用鍵データ K_{STR} 、メディア鍵データ K_{MED} および購入者鍵データ K_{PIN} を順に用いてキーファイル KF_1 内のコンテンツ鍵データ K_c および利用制御状態データ166を暗号化して記録モジュール管理部855に出力する。

そして、記録モジュール管理部855によって、暗号化されたキーファイル KF_1 が、RAM型の記録媒体130₄のセキュアRAM領域132に記録される。

なお、メディア鍵データ K_{MED} は、図33に示す相互認証部170と図32に示すRAM型の記録媒体130₄のメディアSAM133との間の相互認証によって記憶部192に事前に記憶されている。

【0243】

ここで、記録用鍵データ K_{STR} は、例えばSACD (Super Audio Compact Disc)、DVD (Digital Versatile Disc) 機器、CD-R機器およびMD (Mini Disc) 機器などの種類(当該例では、AV機器160₂)に応じて決まるデータであり、機器の種類と記録媒体の種類とを1対1で対応づけるために用いられる。なお、SACDとDVDとでは、ディスク媒体の物理的な構造が同じであるため、DVD機器を用いてSACDの記録媒体の記録・再生を行うことができる場合がある。記録用鍵データ K_{STR} は、このような場合において、不正コピーを防止する役割を果たす。

なお、本実施形態では、記録用鍵データ K_{STR} を用いた暗号化を行わないようにしてもよい。

【0244】

また、メディア鍵データ K_{MED} は、記録媒体(当該例では、RAM型の記録

媒体 130₄) にユニークなデータである。

メディア鍵データ K_{MED} は、記録媒体 (当該例では、図 32 に示す RAM 型の記録媒体 130₄) 側に格納されており、記録媒体のメディア SAM においてメディア鍵データ K_{MED} を用いた暗号化および復号を行うことがセキュリティの観点から好ましい。このとき、メディア鍵データ K_{MED} は、記録媒体にメディア SAM が搭載されている場合には、当該メディア SAM 内に記憶されており、記録媒体にメディア SAM が搭載されていない場合には、例えば、RAM 領域内のホスト CPU 810 の管理外の領域に記憶されている。

なお、本実施形態のように、機器側の SAM (当該例では、SAM105₂) とメディア SAM (当該例では、メディア SAM133) との間で相互認証を行い、セキュアな通信経路を介してメディア鍵データ K_{MED} を機器側の SAM に転送し、機器側の SAM においてメディア鍵データ K_{MED} を用いた暗号化および復号を行なってもよい。

本実施形態では、記録用鍵データ K_{STR} およびメディア鍵データ K_{MED} が、記録媒体の物理層のレベルのセキュリティを保護するために用いられる。

【0245】

また、購入者鍵データ K_{PIN} は、コンテンツファイル CF の購入者を示すデータであり、例えば、コンテンツを買い切りで購入したときに、当該購入したユーザに対して EMD サービスセンタ 102 によって割り当てられる。購入者鍵データ K_{PIN} は、EMD サービスセンタ 102 において管理される。

【0246】

また、上述した実施形態では、記録モジュール 260 を用いて、キーファイル KF , KF_1 を RAM 型の記録媒体 130₄ のセキュア RAM 領域 132 に記録する場合を例示したが、図 32 において点線で示すように、SAM105₂ からメディア SAM133 にキーファイル KF , KF_1 を記録するようにしてもよい。

【0247】

次に、コンテンツの購入形態が未決定の図 12 に示す ROM 型の記録媒体 130₁ をユーザホームネットワーク 303 がオフラインで配給を受けた場合に、A

V機器 160₂ において購入形態を決定する際の処理の流れを図36および図37を参照しながら説明する。

AV機器 160₂ のSAM105₂ は、先ず、図37に示す相互認証部170と図12に示すROM型の記録媒体130₁ のメディアSAM133との間で相互認証を行った後に、メディアSAM133からメディア鍵データ K_{MED} を入力する。

なお、SAM105₂ が、事前にメディア鍵データ K_{MED} を保持している場合には、当該入力を行わなくても良い。

次に、ROM型の記録媒体130₁ のセキュアRAM領域132に記録されているセキュアコンテナ104に格納された図5(B), (C)に示すキーファイルKFおよびその署名データ SIG_7, CP と、公開鍵証明書データ CER_{CP} およびその署名データ SIG_1, ESC とを、メディアSAM管理部197あるいは図示しない読み出しモジュール管理部を介して入力し、これをスタックメモリ200に書き込む。

【0248】

次に、署名処理部189において、署名データ SIG_1, ESC の正当性を確認した後に、公開鍵証明書データ CER_{CP} から公開鍵データ $K_{CP, P}$ を取り出し、この公開鍵データ $K_{CP, P}$ を用いて、署名データ SIG_7, CP の正当性、すなわちキーファイルKFの送信者の正当性を検証する。

また、署名処理部189において、記憶部192から読み出した公開鍵データ $K_{ESC, P}$ を用いて、キーファイルKFに格納された署名データ $SIG_{K1, ESC}$ の正当性、すなわちキーファイルKFの作成者の正当性を検証する。

【0249】

署名処理部189において署名データ $SIG_7, CP, SIG_{K1, ESC}$ の正当性が確認されると、スタックメモリ200からセキュアコンテナ復号部183に、キーファイルKFを読み出す。

次に、セキュアコンテナ復号部183において、対応する期間の配信用鍵データ $KD_1 \sim KD_3$ を用いて、キーファイルKFに格納されたコンテンツ鍵データ Kc 、権利書データ106およびSAMプログラム・ダウンロード・コンテナS

DC₁～SDC₃が復号され、これらがスタックメモリ200に書き込まれる。

【0250】

次に、図37に示す相互認証部170と図36に示す復号・伸長モジュール163との間で相互認証を行った後に、SAM105₂の復号・伸長モジュール管理部184は、スタックメモリ200に記憶されているコンテンツ鍵データK_cおよび権利書データ106に格納された半開示パラメータデータ199、並びにROM型の記録媒体130₁のROM領域131から読み出したコンテンツファイルCFに格納されたコンテンツデータCを図36に示す復号・伸長モジュール163に出力する。次に、復号・伸長モジュール163において、コンテンツデータCがコンテンツ鍵データK_cを用いて半開示モードで復号された後に伸長され、再生モジュール270に出力される。そして、再生モジュール270において、復号・伸長モジュール163からのコンテンツデータCが再生される。

【0251】

次に、ユーザによる図36に示す購入形態決定操作部165の購入操作によってコンテンツの購入形態が決定され、当該決定された購入形態を示す操作信号S165が課金処理部187に入力される。

【0252】

次に、課金処理部187は、操作信号S165に応じた利用制御状態データ166を作成し、これをスタックメモリ200に書き込む。

次に、スタックメモリ200から暗号化・復号部173に、コンテンツ鍵データK_cおよび利用制御状態データ166が出力される。

【0253】

次に、暗号化・復号部173は、スタックメモリ200から入力したコンテンツ鍵データK_cおよび利用制御状態データ166を、記憶部192から読み出した記録用鍵データK_{STR}、メディア鍵データK_{MED}および購入者鍵データK_{PIN}を用いて順次に暗号化してスタックメモリ200に書き込む。

【0254】

次に、メディアSAM管理部197において、スタックメモリ200から読み出した、暗号化されたコンテンツ鍵データK_cおよび利用制御状態データ166

と、SAMプログラム・ダウンロード・コンテナSDC₁～SDC₃を用いて図34(C)に示すキーファイルKF₁が生成される。

また、署名処理部189において、図34(C)に示すキーファイルKF₁のハッシュ値H_{K1}が生成され、当該ハッシュ値H_{K1}がメディアSAM管理部197に出力される。

次に、図37に示す相互認証部170と図36に示すメディアSAM133との間で相互認証を行った後に、メディアSAM管理部197は、キーファイルKF₁およびハッシュ値H_{K1}を、図36に示す記録モジュール271を介してROM型の記録媒体130₁のセキュアRAM領域132に書き込む。

これにより、購入形態が決定されたROM型の記録媒体130₁が得られる。

このとき、課金処理部187が生成した利用制御状態データ166および利用履歴データ108は、所定のタイミングで、スタックメモリ200および外部メモリ201からそれぞれ読み出しされたEMDサービスセンタ102に送信される。

なお、ROM型の記録媒体130₁のメディアSAM133にキーファイルKFが格納されている場合には、図36において点線で示されるように、SAM105₂はメディアSAM133からキーファイルKFを入力する。また、この場合に、SAM105₂は、作成したキーファイルKF₁をメディアSAM133に書き込む。

【0255】

以下、図38に示すように、AV機器160₃において購入形態が未決定のROM型の記録媒体130₁からセキュアコンテナ104を読み出して新たなセキュアコンテナ104_yを生成し、これをAV機器160₂に転送し、AV機器160₂において購入形態を決定してRAM型の記録媒体130₅に書き込む際の処理の流れを図39、図40を参照しながら説明する。

なお、ROM型の記録媒体130₁からRAM型の記録媒体130₅へのセキュアコンテナ104の転送は、図1に示すネットワーク機器160₁およびAV機器160₁～160₄のいずれの間で行ってもよい。

【0256】

まず、AV機器160₃のSAM105₃とROM型の記録媒体130₁のメディアSAM133との間で相互認証を行い、ROM型の記録媒体130₁のメディア鍵データ K_{MED1} をSAM105₃に転送する。

また、AV機器160₂のSAM105₂とRAM型の記録媒体130₅のメディアSAM133との間で相互認証を行い、RAM型の記録媒体130₅メディア鍵データ K_{MED2} をSAM105₂に転送する。

なお、メディア鍵データ K_{MED1} 、 K_{MED2} を用いた暗号化をメディアSAM133およびメディアSAM133において行う場合には、メディア鍵データ K_{MED1} 、 K_{MED2} の転送は行わない。

【0257】

次に、SAM105₃は、図39に示すように、メディアSAM管理部197あるいは図示しない読み出しモジュール管理部を介して、ROM型の記録媒体130₁のROM領域131から読み出した図5(A)に示すコンテンツファイルCFおよびその署名データSIG₆、CPと、セキュアRAM領域132から読み出した図5(B)，(C)に示すキーファイルKFおよびその署名データSIG₇、CPと、公開鍵証明書データCER_{CP}およびその署名データSIG₁，ESCとを、暗号化・復号部171に出力する。

また、メディアSAM管理部197から署名処理部189に、コンテンツファイルCFおよびキーファイルKFが出力される。

そして、署名処理部189において、コンテンツファイルCFおよびキーファイルKFのハッシュ値がとられ、秘密鍵データ K_{SAM3} ，Sを用いて、それぞれ署名データSIG₃₅₀，SAM3，SIG₃₅₂，SAM3が生成され、これらが暗号化・復号部171に出力される。

また、公開鍵証明書データCER_{SAM3}およびその署名データSIG₃₅₁，ESCが記憶部192から読み出されて暗号化・復号部171に出力される。

【0258】

そして、図40に示すセキュアコンテナ104_yが、暗号化・復号部171においてSAM105₃と105₂との間の相互認証によって得られたセッション鍵データ K_{SES} を用いて暗号化された後に、SAM管理部190を介して、A

V機器 160₂ の SAM105₂ に出力される。

【0259】

SAM105₂ では、図41に示すように、SAM管理部190を介してSAM105₃ から入力した図40に示すセキュアコンテナ104_yを暗号化・復号部171においてセッション鍵データK_{SES}を用いて復号した後に、セキュアコンテナ104_y内に格納された署名データSIG₆, CP, SIG₃₅₀, SAM₃の正当性、すなわちコンテンツファイルCFの作成者および送信者の正当性を確認する。

そして、コンテンツファイルCFの作成者および送信者が正当であると確認された後に、メディアSAM管理部197を介してRAM型の記録媒体130₅のRAM領域134にコンテンツファイルCFが書き込まれる。

【0260】

また、SAM管理部190を介してSAM105₃ から入力されたキーファイルKFおよびその署名データSIG₇, CP, SIG₃₅₀, SAM₃と、公開鍵証明書データCER_{SAM3}およびその署名データSIG₃₅₁, ESCとが、スタックメモリ200に書き込まれた後に、暗号化・復号部171においてセッション鍵データK_{SES}を用いて復号される。

次に、当該復号された署名データSIG₃₅₁, ECSが、署名処理部189において署名検証され、公開鍵証明書データCER_{SAM3}の正当性が確認されると、公開鍵証明書データCER_{SAM3}に格納された公開鍵データK_{SAM3}を用いて、署名データSIG₇, CP, SIG₃₅₂, SAM₃の正当性、すなわちキーファイルKFの作成者および送信者の正当性が確認される。

そして、キーファイルKFの作成者および送信者の正当性が確認されると、スタックメモリ200からキーファイルKFが読み出されてセキュアコンテナ復号部183に出力される。

【0261】

次に、セキュアコンテナ復号部183は、対応する期間の配信用鍵データKD₁~KD₃を用いて、キーファイルKFを復号し、当該復号したキーファイルKFをスタックメモリ200に書き込む。

【0262】

次に、スタックメモリ200に記憶されている既に復号されたキーファイルKFに格納された権利書データ106が、利用監視部186に出力される。利用監視部186は、権利書データ106に基づいて、コンテンツの購入形態および利用形態が管理される。

【0263】

次に、例えば、ユーザによって試聴モードが選択されると、既にセッション鍵データK_{SES}で復号されたコンテンツファイルCFのコンテンツデータCと、スタックメモリ200に記憶されたコンテンツ鍵データK_c、権利書データ106から得られた半開示パラメータデータ199およびユーザ電子透かし情報用データ196とが、相互認証を経た後に、図38に示す復号・伸長モジュール管理部184を介して再生モジュール270に出力される。そして、再生モジュール270において、試聴モードに対応したコンテンツデータCの再生が行われる。

【0264】

次に、ユーザによる図38に示す購入・利用形態決定操作部165の操作によってコンテンツの購入・利用形態が決定され、当該決定に応じた操作信号S165が、課金処理部187に出力される。

そして、課金処理部187において、決定された購入・利用形態に応じて利用制御状態データ166および利用履歴データ108が生成され、これがスタックメモリ200および外部メモリ201にそれぞれ書き込まれる。

次に、コンテンツ鍵データK_cおよび利用制御状態データ166が、スタックメモリ200から暗号化・復号部173に読み出され、暗号化・復号部173において記憶部192から読み出した記録用鍵データK_{STR}、メディア鍵データK_{MED2}および購入者鍵データK_{PIN}を用いて順に暗号化され、記録モジュール管理部855に出力される。そして、例えば、記録モジュール管理部855において、図34(C)に示すキーファイルKF₁が作成され、キーファイルKF₁がメディアSAM管理部197を介してRAM型の記録媒体130₅のメディアSAM133に書き込まれる。

また、セキュアコンテナ104_yに格納されたコンテンツファイルCFは、記

録モジュール管理部 855 によって、RAM 型の記録媒体 130₅ の RAM 領域 134 に書き込まれる。

また、利用制御状態データ 166 および利用履歴データ 108 は、所定のタイミングで、EMD サービスセンタ 102 に送信される。

【0265】

以下、SAM105₁～105₄ の実現方法について説明する。

SAM105₁～105₄ の機能をハードウェアとして実現する場合は、メモリを内蔵した ASIC 型の CPU を用いて、そのメモリには、図 26 に示す各機能を実現するためのセキュリティー機能モジュールやコンテンツの権利処理をおこなうプログラムモジュールおよび鍵データなどの機密度の高いデータが格納される。暗号ライブラリーモジュール（公開鍵暗号、共通鍵暗号、乱数発生器、ハッシュ関数）、コンテンツの使用制御用のプログラムモジュール、課金処理のプログラムモジュールなど、一連の権利処理用のプログラムモジュールは、例えば、ソフトウェアとして実装される。

【0266】

例えば、図 26 に示す暗号化・復号部 171 などのモジュールは、例えば、処理速度の問題でハードウェアとして ASIC 型の CPU 内の IP コアとして実装される。クロック速度や CPU コード体系などの性能によっては、暗号化・復号部 171 をソフトウェアとして実装してもよい。

また、図 26 に示す記憶部 192 や、図 26 に示す機能を実現するためのプログラムモジュールおよびデータを格納するメモリとしては、例えば、不揮発メモリ（フラッシュ ROM）が用いられ、作業用メモリとしては SRAM などの高速書き込み可能なメモリが用いられる。なお、その他にも、SAM105₁～105₄ に内蔵されるメモリとして、強誘電体メモリ（FeRAM）を用いてもよい。

また、SAM105₁～105₄ には、その他に、コンテンツの利用のための有効期限や契約期間などで日時の検証に使用する時計機能が内蔵されている。

【0267】

上述したように、SAM105₁～105₄ は、プログラムモジュールや、デ

ータおよび処理内容を外部から遮蔽した耐タンパ性の構造を持っている。SAM 105₁～105₄を搭載した機器のホストCPUのバス経由で、当該SAMのIC内部のメモリに格納されている秘密性の高いプログラムおよびデータの内容や、SAMのシステムコンフィギュレーション (System Configuration) 関連のレジスタ群および暗号ライブラリーや時計のレジスタ群などの値が、読み出されたり、新規に書き込まれたりしないように、すなわち、搭載機器のホストCPUが割り付けているアドレス空間内に存在しないように、当該SAMでは、CPU側のメモリー空間を管理するMMU (Memory Management Unit) を用いて、搭載機器側のホストCPUからは見えないアドレス空間を設定する。

また、SAM105₁～105₄は、X線や熱などの外部からの物理的な攻撃にも耐え得る構造をもち、さらにデバッグ用ツール (ハードウェアICE、ソフトウェアICE) などを用いたリアルタイムデバッグ (リバースエンジニアリング) が行われても、その処理内容が分からないか、あるいは、デバッグ用ツールそのものがIC製造後には使用できないような構造をしている。

SAM105₁～105₄自身は、ハードウェア的な構造においては、メモリを内蔵した通常のASIC型のCPUであり、機能は当該CPUを動作させるソフトウェアに依存するが、暗号機能と耐タンパ性のハードウェア構造を有している点が、一般的なASIC型のCPUと異なる。

【0268】

SAM105₁～105₄の機能を全てソフトウェアで実現する場合は、耐タンパ性を持ったモジュール内部で閉じてソフトウェア処理をおこなう場合と、通常のセットに搭載されているホストCPU上のソフトウェア処理で行い、当該処理のときにのみ解読することが不可能となる仕掛けをする場合とがある。前者は、暗号ライブラリモジュールがIPコアではなく、通常のソフトウェアモジュールとしてメモリに格納される場合と同じであり、ハードウェアとして実現する場合と同様に考えられる。一方、後者は、タンパーレジスタントソフトウェアと呼ばれるもので、ICE (デバッガ) で実行状況を解読されても、そのタスクの実行順序がバラバラであったり (この場合には、区切ったタスク単体でプログラム

としての意味があるように、すなわち前後のラインに影響がでないようにタスク切りを行う)、タスクそのものが暗号化されており、一種のセキュア処理を目的としたタスクスケジューラ (Mini OS) と同様に実現できる。当該タスクスケジューラは、ターゲットプログラムに埋め込まれている。

【0269】

次に、図25に示す復号・伸長モジュール163について説明する。

図25に示すように、復号・伸長モジュール163は、相互認証部220、復号部221、復号部222、伸長部223、電子透かし情報処理部224および半開示処理部225を有する。

相互認証部220は、復号・伸長モジュール163がSAM105₁からデータを入力する際に、図32に示す相互認証部170との間で相互認証を行ってセッション鍵データK_{SES}を生成する。

【0270】

復号部221は、SAM105₁から入力したコンテンツ鍵データK_c、半開示パラメータデータ199、ユーザ電子透かし情報用データ196およびコンテンツデータCを、セッション鍵データK_{SES}を用いて復号する。そして、復号部221は、復号したコンテンツ鍵データK_cおよびコンテンツデータCを復号部222に出力し、復号したユーザ電子透かし情報用データ196を電子透かし情報処理部224に出力し、半開示パラメータデータ199を半開示処理部225に出力する。

【0271】

復号部222は、半開示処理部225からの制御に基づいて、コンテンツ鍵データK_cを用いて、コンテンツデータCを半開示状態で復号し、復号したコンテンツデータCを伸長部223に出力する。

【0272】

伸長部223は、復号されたコンテンツデータCを伸長して、電子透かし情報処理部224に出力する。

伸長部223は、例えば、図5(A)に示すコンテンツファイルCFに格納されたA/V伸長用ソフトウェアを用いて伸長処理を行い、例えば、ATRAC3

方式で伸長処理を行う。

【0273】

電子透かし情報処理部224は、復号されたユーザ電子透かし情報用データ196に応じたユーザ電子透かし情報を、復号されたコンテンツデータCに埋め込み、新たなコンテンツデータCを生成する。電子透かし情報処理部224は、当該新たなコンテンツデータCを再生モジュール169に出力する。

このように、ユーザ電子透かし情報は、コンテンツデータCを再生するとき、復号・伸長モジュール163において埋め込まれる。

なお、本発明では、コンテンツデータCにユーザ電子透かし情報用データ196を埋め込まないようにしてもよい。

【0274】

半開示処理部225は、半開示パラメータデータ199に基づいて、例えば、コンテンツデータCのうち復号を行わないブロックと、復号を行うブロックとを復号部222に指示する。

また、半開示処理部225は、その他に、半開示パラメータデータ199に基づいて、試聴時の再生機能を限定したり、試聴可能な期間を限定するなどの制御を行う。

【0275】

再生モジュール169は、復号および伸長されたコンテンツデータCに応じた再生を行う。

【0276】

次に、コンテンツプロバイダ101、EMDサービスセンタ102およびユーザホームネットワーク103の間で、秘密鍵データを用いて生成した署名データを付したデータおよび公開鍵証明書データを送受信する際のデータフォーマットについて説明する。

図42(A)は、コンテンツプロバイダ101からSAM105₁にデータDataをイン・バンド方式で送信する場合のデータフォーマットを説明するための図である。

この場合には、コンテンツプロバイダ101からSAM105₁に、コンテン

ツプロバイダ101とSAM105₁との間の相互認証によって得たセッション鍵データ K_{SES} で暗号化したモジュールMod₅₀が送信される。

モジュールMod₅₀には、モジュールMod₅₁およびその秘密鍵データ $K_{CP, S}$ による署名データ SIG_{CP} が格納されている。

モジュールMod₅₁には、コンテンツプロバイダ101の秘密鍵データ $K_{CP, P}$ を格納した公開鍵証明書データ CER_{CP} と、公開鍵証明書データ CER_{CP} に対しての秘密鍵データ $K_{ESC, S}$ による署名データ SIG_{ESC} と、送信するデータDataとが格納されている。

このように、公開鍵証明書データ CER_{CP} を格納したモジュールMod₅₀を、コンテンツプロバイダ101からSAM105₁に送信することで、SAM105₁において署名データ SIG_{CP} の検証を行なう際に、EMDサービスセンタ102からSAM105₁に公開鍵証明書データ CER_{CP} を送信する必要がなくなる。

【0277】

図42 (B), (C) は、コンテンツプロバイダ101からSAM105₁にデータDataをアウト・オブ・バンド方式で送信する場合のデータフォーマットを説明するための図である。

この場合には、コンテンツプロバイダ101からSAM105₁に、コンテンツプロバイダ101とSAM105₁との間の相互認証によって得たセッション鍵データ K_{SES} で暗号化した図42 (B) に示すモジュールMod₅₂が送信される。

モジュールMod₅₂には、送信するデータDataと、その秘密鍵データ $K_{CP, S}$ による署名データ SIG_{CP} とが格納されている。

また、EMDサービスセンタ102からSAM105₁には、EMDサービスセンタ102とSAM105₁との間の相互認証によって得たセッション鍵データ K_{SES} で暗号化した図42 (C) に示すモジュールMod₅₃が送信される。

モジュールMod₅₃には、コンテンツプロバイダ101の公開鍵証明書データ CER_{CP} と、その秘密鍵データ $K_{ESC, S}$ による署名データ SIG_{ESC}

とが格納されている。

【0278】

図42(D)は、SAM105₁からコンテンツプロバイダ101にデータDataをイン・バンド方式で送信する場合のデータフォーマットを説明するための図である。

この場合には、SAM105₁からコンテンツプロバイダ101に、コンテンツプロバイダ101とSAM105₁との間の相互認証によって得たセッション鍵データK_{SES}で暗号化したモジュールMod₅₄が送信される。

モジュールMod₅₄には、モジュールMod₅₅およびその秘密鍵データK_{SAM1, S}による署名データSIG_{SAM1}が格納されている。

モジュールMod₅₅には、SAM105₁の秘密鍵データK_{SAM1, P}を格納した公開鍵証明書データCER_{SAM1}と、公開鍵証明書データCER_{SAM1}に対しての秘密鍵データK_{ESC, S}による署名データSIG_{ESC}と、送信するデータDataとが格納されている。

このように、公開鍵証明書データCER_{SAM1}を格納したモジュールMod₅₅を、SAM105₁からコンテンツプロバイダ101に送信することで、コンテンツプロバイダ101において署名データSIG_{SAM1}の検証を行なう際に、EMDサービスセンタ102からコンテンツプロバイダ101に公開鍵証明書データCER_{SAM1}を送信する必要がなくなる。

【0279】

図42(E), (F)は、SAM105₁からコンテンツプロバイダ101にデータDataをアウト・オブ・バンド方式で送信する場合のデータフォーマットを説明するための図である。

この場合には、SAM105₁からコンテンツプロバイダ101に、コンテンツプロバイダ101とSAM105₁との間の相互認証によって得たセッション鍵データK_{SES}で暗号化した図42(E)に示すモジュールMod₅₆が送信される。

モジュールMod₅₆には、送信するデータDataと、その秘密鍵データK_{SAM1, S}による署名データSIG_{SAM1}とが格納されている。

また、EMDサービスセンタ102からコンテンツプロバイダ101には、EMDサービスセンタ102とコンテンツプロバイダ101との間の相互認証によって得たセッション鍵データ K_{SES} で暗号化した図42(F)に示すモジュールMod₅₇が送信される。

モジュールMod₅₇には、SAM105₁の公開鍵証明書データ CER_{SAM1} と、その秘密鍵データ $K_{ESC, S}$ による署名データ SIG_{ESC} とが格納されている。

【0280】

図43(G)は、コンテンツプロバイダ101からEMDサービスセンタ102にデータDataをイン・バンド方式で送信する場合のデータフォーマットを説明するための図である。

この場合には、コンテンツプロバイダ101からEMDサービスセンタ102に、コンテンツプロバイダ101とEMDサービスセンタ102との間の相互認証によって得たセッション鍵データ K_{SES} で暗号化したモジュールMod₅₈が送信される。

モジュールMod₅₈には、モジュールMod₅₉およびその秘密鍵データ $K_{CP, S}$ による署名データ SIG_{CP} が格納されている。

モジュールMod₅₉には、コンテンツプロバイダ101の秘密鍵データ $K_{CP, P}$ を格納した公開鍵証明書データ CER_{CP} と、公開鍵証明書データ CER_{CP} に対しての秘密鍵データ $K_{ESC, S}$ による署名データ SIG_{ESC} と、送信するデータDataとが格納されている。

【0281】

図43(H)は、コンテンツプロバイダ101からEMDサービスセンタ102にデータDataをアウト・オブ・バンド方式で送信する場合のデータフォーマットを説明するための図である。

この場合には、コンテンツプロバイダ101からEMDサービスセンタ102に、コンテンツプロバイダ101とEMDサービスセンタ102との間の相互認証によって得たセッション鍵データ K_{SES} で暗号化した図43(H)に示すモジュールMod₆₀が送信される。

モジュールMod₆₀には、送信するデータDataと、その秘密鍵データK_{CP, S}による署名データSIG_{CP}とが格納されている。

このとき、EMDサービスセンタ102にはコンテンツプロバイダ101の公開鍵証明書データCER_{CP}は既に登録されている。

【0282】

図43 (I) は、SAM105₁からEMDサービスセンタ102にデータDataをイン・バンド方式で送信する場合のデータフォーマットを説明するための図である。

この場合には、SAM105₁からEMDサービスセンタ102に、EMDサービスセンタ102とSAM105₁との間の相互認証によって得たセッション鍵データK_{SES}で暗号化したモジュールMod₆₁が送信される。

モジュールMod₆₁には、モジュールMod₆₂およびその秘密鍵データK_{SAM1, S}による署名データSIG_{SAM1}が格納されている。

モジュールMod₆₂には、SAM105₁の秘密鍵データK_{SAM1, P}を格納した公開鍵証明書データCER_{SAM1}と、公開鍵証明書データCER_{SAM1}に対しての秘密鍵データK_{ESC, S}による署名データSIG_{ESC}と、送信するデータDataとが格納されている。

【0283】

図43 (J) は、SAM105₁からEMDサービスセンタ102にデータDataをアウト・オブ・バンド方式で送信する場合のデータフォーマットを説明するための図である。

この場合には、SAM105₁からEMDサービスセンタ102に、EMDサービスセンタ102とSAM105₁との間の相互認証によって得たセッション鍵データK_{SES}で暗号化した図43 (J) に示すモジュールMod₆₃が送信される。

モジュールMod₆₃には、送信するデータDataと、その秘密鍵データK_{SAM1, S}による署名データSIG_{SAM1}とが格納されている。

このとき、EMDサービスセンタ102にはSAM105₁の公開鍵証明書データCER_{SAM1}は既に登録されている。

【0284】

以下、SAM105₁～105₄の出荷時におけるEMDサービスセンタ102への登録処理について説明する。

なお、SAM105₁～105₄の登録処理は同じであるため、以下、SAM105₁の登録処理について述べる。

SAM105₁の出荷時には、図24に示すEMDサービスセンタ102の鍵サーバ141によって、SAM管理部149を介して、図26などに示す記憶部192に以下に示す鍵データが初期登録される。

また、SAM105₁には、例えば、出荷時に、記憶部192などに、SAM105₁がEMDサービスセンタ102に初回にアクセスする際に用いられるプログラムなどが記憶される。

すなわち、記憶部192には、例えば、図30において左側に「*」が付されているSAM105₁の識別子SAM_ID、記録用鍵データK_{STR}、ルート認証局2の公開鍵データK_{R-CA}、EMDサービスセンタ102の公開鍵データK_{ESC, P}、SAM105₁の秘密鍵データK_{SAM1, S}、公開鍵証明書データCER_{SAM1}およびその署名データSIG_{22, ESC}、復号・伸長モジュール163およびメディアSAMとの間の認証用鍵データを生成するための元鍵データが初期登録で記憶される。

なお、公開鍵証明書データCER_{SAM1}は、SAM105₁を出荷後に登録する際にEMDサービスセンタ102からSAM105₁に送信してもよい。

【0285】

また、記憶部192には、SAM105₁の出荷時に、図5に示すコンテンツファイルCFおよびキーファイルKFを読み込み形式を示すファイルリーダーが、EMDサービスセンタ102によって書き込まれる。

SAM105₁では、コンテンツファイルCFおよびキーファイルKFに格納されたデータを利用する際に、記憶部192に記憶されたファイルリーダーが用いられる。

【0286】

ここで、ルート認証局2の公開鍵データK_{R-CA}は、インターネットの電子

商取引などでは一般的に使用されているRSAを使用し、データ長は例えば1024ビットである。公開鍵データ K_{R-CA} は、図1に示すルート認証局2によって発行される。

また、EMDサービスセンタ102の公開鍵データ $K_{ESC, P}$ は、短いデータ長でRSAと同等あるいはそれ以上の強度を持つ楕円曲線暗号を利用して生成され、データ長は例えば160ビットである。但し、暗号化の強度を考慮すると、公開鍵データ $K_{ESC, P}$ は192ビット以上であることが望ましい。また、EMDサービスセンタ102は、ルート認証局92に公開鍵データ $K_{ESC, P}$ を登録する。

また、ルート認証局92は、公開鍵データ $K_{ESC, P}$ の公開鍵証明書データ CER_{ESC} を作成する。公開鍵データ $K_{ESC, P}$ を格納した公開鍵証明書データ CER_{ESC} は、好ましく、SAM105₁の出荷時に記憶部192に記憶される。この場合に、公開鍵証明書データ CER_{ESC} は、ルート認証局92の秘密鍵データ $K_{ROOT, S}$ で署名されている。

【0287】

EMDサービスセンタ102は、乱数を発生してSAM105₁の秘密鍵データ $K_{SAM1, S}$ を生成し、これとペアとなる公開鍵データ $K_{SAM1, P}$ を生成する。

また、EMDサービスセンタ102は、ルート認証局92の認証をもらって、公開鍵データ $K_{SAM1, P}$ の公開鍵証明書データ CER_{SAM1} を発行し、これに自らの秘密鍵データ $K_{ESC, S}$ を用いて署名データを添付する。すなわち、EMDサービスセンタ102は、セカンドCA（認証局）として機能を果たす。

【0288】

また、SAM105₁には、図24に示すEMDサービスセンタ102のSAM管理部149により、EMDサービスセンタ102の管理下にある一意（ユニーク）な識別子SAM_IDが割り当てられ、これがSAM105₁の記憶部192に格納されると共に、図24に示すSAMデータベース149aにも格納され、EMDサービスセンタ102によって管理される。

【0289】

また、SAM105₁は、出荷後、例えば、ユーザによってEMDサービスセンタ102と接続され、登録手続を行うと共に、EMDサービスセンタ102から記憶部192に配信用鍵データKD₁～KD₃が転送される。

すなわち、SAM105₁を利用するユーザは、コンテンツをダウンロードする前にEMDサービスセンタ102に登録手続が必要である。この登録手続は、例えば、SAM105₁を搭載している機器（当該例では、ネットワーク機器160₁）を購入したときに添付された登録用紙などを用いて、ユーザ本人が自己を特定する情報を記載して例えば郵便などのオフラインで行なわれる。

SAM105₁は、上述した登録手続を経た後でないと使用できない。

【0290】

EMDサービスセンタ102は、SAM105₁のユーザによる登録手続に応じて、ユーザに固有の識別子USER_IDを発行し、例えば、図24に示すSAMデータベース149aにおいて、SAM_IDとUSER_IDとの対応関係を管理し、課金時に利用する。

また、EMDサービスセンタ102は、SAM105₁のユーザに対して情報参照用識別子IDと、初回に使用されるパスワードを割り当て、これをユーザに通知する。ユーザは、情報参照用識別子IDとパスワードとを用いて、EMDサービスセンタ102に、例えば現在までのコンテンツデータの利用状況（利用履歴）などを情報の問い合わせを行なうことができる。

また、EMDサービスセンタ102は、ユーザの登録時に、クレジットカード会社などに身分の確認を行なったり、オフラインで本人の確認を行なう。

【0291】

次に、図30に示すように、SAM105₁内の記憶部192にSAM登録リストを格納する手順について説明する。

図1に示すSAM105₁は、例えば、バス191としてIEEE1394シリアルバスを用いた場合に、バス191に接続された機器の電源を立ち上げたり、新しい機器をバス191に接続したときに生成されるトポロジーマップを利用して、自分の系に存在するSAM105₂～SAM105₄のSAM登録リスト

を得る。

なお、IEEE 1394 シリアルバスであるバス 191 に応じて生成されたトポロジーマップは、例えば、図 44 に示すように、バス 191 に SAM105₁ ~ 105₄ に加えて AV 機器 160₅, 160₆ の SCMS 処理回路 105₅, 105₆ が接続されている場合に、SAM105₁ ~ 105₄ および SCMS 処理回路 105₅, 105₆ を対象として生成される。

従って、SAM105₁ は、当該トポロジーマップから、SAM105₁ ~ 105₄ についての情報を抽出して図 45 に示す SAM 登録リストを生成する。

【0292】

そして、SAM105₁ は、図 45 に示す SAM 登録リストを、EMD サービスセンタ 102 に登録して署名を得る。

これらの処理は、バス 191 のセッションを利用して SAM105₁ が自動的に
に行い、EMD サービスセンタ 102 に SAM 登録リストの登録命令を発行する
。

EMD サービスセンタ 102 は、SAM105₁ から図 45 に示す SAM 登録リストを受けると、有効期限を確認する。そして、EMD サービスセンタ 102 は、登録時に SAM105₁ より指定された決済機能の有無を参照して対応する部分の設定を行う。また、EMD サービスセンタ 102 は、リボケーションリストをチェックして SAM 登録リスト内のリボケーションフラグを設定する。リボケーションリストは、例えば、不正使用などを理由に EMD サービスセンタ 102 によって使用が禁止されている（無効な）SAM のリストである。

また、EMD サービスセンタ 102 は、決済時には SAM105₁ に対応する SAM 登録リストを取り出し、その中に記述された SAM がリボケーションリストに含まれているかを確認する。また、EMD サービスセンタ 102 は、SAM 登録リストに署名を添付する。

これにより、図 46 に示す SAM 登録リストが作成される。

なお、SAM リボケーションリストは、同一系の（同一のバス 191 に接続されている）SAM のみを対象として生成され、各 SAM に対応するリボケーションフラグによって、当該 SAM の有効および無効を示している。

【0293】

以下、図1に示すコンテンツプロバイダ101の全体動作について説明する。

図47は、コンテンツプロバイダ101の全体動作のフローチャートである。

ステップS1：EMDサービスセンタ102は、コンテンツプロバイダ101が所定の登録処理を経た後に、コンテンツプロバイダ101の公開鍵データ K_{CP} 、 P の公開鍵証明書 CER_{CP} をコンテンツプロバイダ101に送信する。

また、EMDサービスセンタ102は、 $SAM105_1 \sim 105_4$ が所定の登録処理を経た後に、 $SAM105_1 \sim 105_4$ の公開鍵データ $K_{SAM1, P} \sim K_{SAM4, P}$ の公開鍵証明書 $CER_{CP1} \sim CER_{CP4}$ を $SAM105_1 \sim 105_4$ に送信する。

また、EMDサービスセンタ102は、相互認証を行った後に、各々有効期限が1カ月の3カ月分の配信用鍵データ $KD_1 \sim KD_3$ をユーザホームネットワーク103の $SAM105_1 \sim 105_4$ に送信する。

このように、EMDシステム100では、配信用鍵データ $KD_1 \sim KD_3$ を予め $SAM105_1 \sim 105_4$ に配給しているため、 $SAM105_1 \sim 105_4$ とEMDサービスセンタ102との間がオフラインの状態でも、 $SAM105_1 \sim 105_4$ においてコンテンツプロバイダ101から配給されたセキュアコンテンツ104を復号して購入・利用できる。この場合に、当該購入・利用の履歴は利用履歴データ108に記述され、利用履歴データ108は、 $SAM105_1 \sim 105_4$ とEMDサービスセンタ102とが接続されたときに、EMDサービスセンタ102に自動的に送信されるため、EMDサービスセンタ102における決済処理を確実に行うことができる。なお、EMDサービスセンタ102が、所定の期間内に、利用履歴データ108を回収できないSAMについては、リボケーションリストで無効の対象とする。

なお、利用制御状態データ166は、原則として、リアルタイムで、 $SAM105_1 \sim 105_4$ からEMDサービスセンタ102に送信される。

【0294】

ステップS2：コンテンツプロバイダ101は、相互認証を行った後に、図18に示す登録用モジュール Mod_2 を、EMDサービスセンタ102に送信する

そして、EMDサービスセンタ102は、所定の署名検証を行った後に、権利書データ106およびコンテンツ鍵データKcを登録して権威化する。

また、EMDサービスセンタ102は、登録用モジュールMod₂に応じた6カ月分のキーファイルKFを作成し、これをコンテンツプロバイダ101に送信する。

【0295】

ステップS3：コンテンツプロバイダ101は、図5（A）、（B）に示すコンテンツファイルCFおよびその署名データSIG₆, CPと、キーファイルKFおよびその署名データSIG₇, CPとを作成し、これらと図5（C）に示す公開鍵証明書データCER_{cp}およびその署名データSIG₁, ESCとを格納したセキュアコンテナ104を、オンラインおよび／またはオフラインで、ユーザホームネットワーク103のSAM105₁～105₄に配給する。

オンラインの場合には、コンテンツプロバイダ用配送プロトコルを用いられ、当該プロトコルに依存しない形式で（すなわち、複数階層からなる通信プロトコルの所定の層を用いて伝送されるデータとして）、セキュアコンテナ104がコンテンツプロバイダ101からユーザホームネットワーク103に配送される。また、オフラインの場合には、ROM型あるいはRAM型の記録媒体に記録された状態で、セキュアコンテナ104が、コンテンツプロバイダ101からユーザホームネットワーク103に配送される。

【0296】

ステップS4：ユーザホームネットワーク103のSAM105₁～SAM105₄は、コンテンツプロバイダ101から配給を受けたセキュアコンテナ104内の署名データSIG₆, CP, SIG₇, CP, SIG_{K1}, ESCを検証して、コンテンツファイルCFおよびキーファイルKFの作成者および送信者の正当性を確認した後に、対応する期間の配信用鍵データKD₁～KD₆を用いてキーファイルKFを復号する。

【0297】

ステップS5：SAM105₁～SAM105₄において、ユーザによる図2

5に示す購入・利用形態決定操作部165の操作に応じた操作信号S165に基づいて、購入・利用形態を決定する。

このとき、図31に示す利用監視部186において、セキュアコンテナ104に格納された権利書データ106に基づいて、ユーザによるコンテンツファイルCFの購入・利用形態が管理される。

【0298】

ステップS6：SAM105₁～SAM105₄の図31に示す課金処理部187において、操作信号S165に基づいて、ユーザによる購入・利用形態の決定の操作を記述した利用履歴データ108および利用制御状態データ166が生成し、これらをEMDサービスセンタ102に送信する。

【0299】

ステップS7：EMDサービスセンタ102は、図24に示す決算処理部142において、利用履歴データ108に基づいて決済処理を行い、決済請求権データ152および決済レポートデータ107を作成する。EMDサービスセンタ102は、決済請求権データ152およびその署名データSIG_gを、図1に示すペイメントゲートウェイ90を介して、決済機関91に送信する。また、EMDサービスセンタ102は、決済レポートデータ107をコンテンツプロバイダ101に送信する。

【0300】

ステップS8： 決済機関91において、署名データSIG_gの検証を行った後に、決済請求権データ152に基づいて、ユーザが支払った金額が、コンテンツプロバイダ101の所有者に分配される。

【0301】

以上説明したように、EMDシステム100では、図5に示すフォーマットのセキュアコンテナ104をコンテンツプロバイダ101からユーザホームネットワーク103に配給し、セキュアコンテナ104内のキーファイルKFについての処理をSAM105₁～105₄内で行う。

また、キーファイルKFに格納されたコンテンツ鍵データKcおよび権利書データ106は、配信鍵データKD₁～KD₃を用いて暗号化されており、配信鍵

データKD₁～KD₃を保持しているSAM105₁～105₄内でのみ復号される。そして、SAM105₁～105₄では、耐タンパ性を有するモジュールであり、権利書データ106に記述されたコンテンツデータCの取り扱い内容に基づいて、コンテンツデータCの購入形態および利用形態が決定される。

従って、EMDシステム100によれば、ユーザホームネットワーク103におけるコンテンツデータCの購入および利用を、コンテンツプロバイダ101の関係者が作成した権利書データ106の内容に基づいて確実に行わせることができる。

【0302】

また、EMDシステム100では、コンテンツプロバイダ101からユーザホームネットワーク103へのコンテンツデータCの配給を、オンラインおよびオフラインの何れの場合でもセキュアコンテナ104を用いて行うことで、SAM105₁～105₄におけるコンテンツデータCの権利処理を双方の場合において共通化できる。

【0303】

また、EMDシステム100では、ユーザホームネットワーク103内のネットワーク機器160₁およびAV機器160₂～160₄においてコンテンツデータCを購入、利用、記録および転送する際に、常に権利書データ106に基づいて処理を行うことで、共通の権利処理ルールを採用できる。

【0304】

図48は、第1実施形態で採用されるセキュアコンテナの配送プロトコルの一例を説明するための図である。

図48に示すように、マルチプロセッサシステム100では、コンテンツプロバイダ101からユーザホームネットワーク103にセキュアコンテナ104を配送するプロトコルとして例えばTCP/IPおよびXML/SMILが用いられる。

また、ユーザホームネットワーク103のSAM相互間でセキュアコンテナを転送するプロトコル、並びにユーザホームネットワーク103と103aとの間でセキュアコンテナを転送するプロトコルとして例えば1394シリアルバス・

インタフェース上に構築されたXML/SMILが用いられる。また、この場合に、ROM型やRAM型の記録媒体にセキュアコンテナを記録してSAM相互間で配送してもよい。

【0305】

第1実施形態の第1変形例

上述した実施形態では、図5(B)に示すように、EMDサービスセンタ102において配信用鍵データKDを用いてキーファイルKFを暗号化し、SAM105₁～105₄において配信用鍵データKDを用いてキーファイルKFを復号する場合を例示したが、図1に示すように、コンテンツプロバイダ101からSAM105₁～105₄にセキュアコンテナ104を直接供給する場合には、配信用鍵データKDを用いたキーファイルKFの暗号化は必ずしも行なわなくてもよい。

このように、配信用鍵データKDを用いてキーファイルKFを暗号化することは、後述する第2実施形態のように、コンテンツプロバイダからユーザホームネットワークにサービスプロバイダを介してコンテンツデータを供給する場合に、配信用鍵データKDをコンテンツプロバイダおよびユーザホームネットワークにのみ保持させることで、サービスプロバイダによる不正行為を抑制する際に大きな効果を発揮する。

但し、上述した第1実施形態の場合でも、配信用鍵データKDを用いてキーファイルKFを暗号化することは、コンテンツデータの不正利用の抑制力を高める点で効果がある。

【0306】

また、上述した実施形態では、図5(B)に示すキーファイルKF内の権利書データ106内に標準小売価格データSRPを格納する場合を例示したが、セキュアコンテナ104内のキーファイルKFの外に、標準小売価格データSRP（プライスタグデータ）を格納してもよい。この場合には、標準小売価格データSRPに対して秘密鍵データK_{c_p}を用いて作成した署名データを添付する。

【0307】

第1実施形態の第2変形例

上述した第1実施形態では、図1に示すように、EMDサービスセンタ102が、自らが生成した決済請求権データ152を用いて、ペイメントゲートウェイ90を介して決済機関91で決済処理を行なう場合を例示したが、例えば、図49に示すように、EMDサービスセンタ102からコンテンツプロバイダ101に決済請求権データ152を送信し、コンテンツプロバイダ101自らが、決済請求権データ152を用いて、ペイメントゲートウェイ90を介して決済機関91に対して決済処理を行なってもよい。

【0308】

第1実施形態の第3変形例

上述した第1実施形態では、単数のコンテンツプロバイダ101からユーザホームネットワーク103のSAM105₁～105₄に、セキュアコンテナ104を供給する場合を例示したが、2以上のコンテンツプロバイダ101a, 101bからSAM105₁～105₄にそれぞれセキュアコンテナ104a, 104bを供給するようにしてもよい。

図50は、コンテンツプロバイダ101a, 101bを用いる場合の第1実施形態の第3変形例に係わるEMDシステムの構成図である。

この場合には、EMDサービスセンタ102は、コンテンツプロバイダ101aおよび101bに、それぞれの6カ月分の配信用鍵データKD a₁～KD a₆およびKD b₁～KD b₆を用いて暗号化したキーファイルKF a₁～KF a₆およびKF b₁～KF b₆を配信する。

また、EMDサービスセンタ102は、SAM105₁～105₄に、3カ月分の配信用鍵データKD a₁～KD a₃およびKD b₁～KD b₃を配信する。

【0309】

そして、コンテンツプロバイダ101aは、独自のコンテンツ鍵データKc aを用いて暗号化したコンテンツファイルCF aと、EMDサービスセンタ102から受信した対応する期間のキーファイルKF a₁～KF a₆とを格納したセキュアコンテナ104aをSAM105₁～105₄にオンラインおよび／またはオフランで供給する。

このとき、キーファイルの識別子として、EMDサービスセンタ102が配付

するグローバルユニークな識別子コンテンツIDが用いられ、EMDサービスセンタ102によって、コンテンツデータが一元的に管理される。

また、コンテンツプロバイダ101bは、独自のコンテンツ鍵データKcbを用いて暗号化したコンテンツファイルCFbと、EMDサービスセンタ102から受信した対応する期間のキーファイルKFb₁～KFb₆とを格納したセキュアコンテナ104bをSAM105₁～105₄にオンラインおよび／またはオフランで供給する。

【0310】

SAM105₁～105₄は、セキュアコンテナ104aについては、対応する期間の配信用鍵データKDa₁～KDa₃を用いて復号を行い、所定の署名検証処理などを経てコンテンツの購入形態を決定し、当該決定された購入形態および利用形態などに応じて生成した利用履歴データ108aおよび利用制御状態データ166aをEMDサービスセンタ102に送信する。

また、SAM105₁～105₄は、セキュアコンテナ104bについては、対応する期間の配信用鍵データKDb₁～KDb₃を用いて復号を行い、所定の署名検証処理などを経てコンテンツの購入形態を決定し、当該決定された購入形態および利用形態などに応じて生成した利用履歴データ108bおよび利用制御状態データ166bをEMDサービスセンタ102に送信する。

【0311】

EMDサービスセンタ102では、利用履歴データ108aに基づいて、コンテンツプロバイダ101aについての決済請求権データ152aを作成し、これを用いて決済機関91に対して決済処理を行なう。

また、EMDサービスセンタ102では、利用履歴データ108bに基づいて、コンテンツプロバイダ101bについての決済請求権データ152bを作成し、これを用いて決済機関91に対して決済処理を行なう。

【0312】

また、EMDサービスセンタ102は、権利書データ106a, 106bを登録して権威化を行なう。このとき、EMDサービスセンタ102は、権利書データ106a, 106bに対応するキーファイルKFa, KFbに対して、グロー

バルユニークな識別子コンテンツIDを配付する。

また、EMDサービスセンタ102は、コンテンツプロバイダ101a, 101bの公開鍵証明書データ CER_{cpa} , CER_{CPb} を発行し、これに自らの署名データ SIG_{1b} , ESC , SIG_{1a} , ESC を付してその正当性を認証する。

【0313】

第1実施形態の第4変形例

上述した実施形態では、コンテンツファイルCFおよびキーファイルKFをディレクトリ構造でセキュアコンテナ104内に格納してコンテンツプロバイダ101から $SAM105_1 \sim 105_4$ に送信する場合を例示したが、コンテンツファイルCFおよびキーファイルKFを、別々に $SAM105_1 \sim 105_4$ に送信してもよい。

これには、例えば、以下に示す第1の手法と第2の手法とがある。

第1の手法では、図51に示すように、コンテンツプロバイダ101から $SAM105_1 \sim 105_4$ に、通信プロトコルに依存しない形式で、コンテンツファイルCFおよびキーファイルKFを別々に送信する。

また、第2の手法では、図52に示すように、コンテンツプロバイダ101から $SAM105_1 \sim 105_4$ にコンテンツファイルCFを通信プロトコルに依存しない形式で送信すると共に、EMDサービスセンタ102から $SAM105_1 \sim 105_4$ にキーファイルKFを送信する。当該キーファイルKFの送信は、例えば、 $SAM105_1 \sim 105_4$ のユーザが、コンテンツデータCの購入形態を決定しようとするときに、EMDサービスセンタ102から $SAM105_1 \sim 105_4$ に送信される。

上述した第1の手法および第2の手法を採用する場合には、関連するコンテンツファイルCF相互間と、コンテンツファイルCFとそれに対応するキーファイルKFとの間を、コンテンツファイルCFおよびキーファイルKFの少なくとも一方のヘッダに格納されたハイパーリンクデータを用いてリンク関係を確立する。 $SAM105_1 \sim 105_4$ では、当該リンク関係に基づいて、コンテンツデータCの権利処理および利用を行う。

なお、本変形例において、コンテンツファイルCFおよびキーファイルKFのフォーマットは、例えば、図5(A)，(B)に示すものが採用される。また、この場合に、コンテンツファイルCFおよびキーファイルKFと共に、それらの署名データSIG₆，CP，SIG₇，CPを送信することが好ましい。

第1実施形態の第5変形例

上述した実施形態では、セキュアコンテナ104内において、コンテンツファイルCFおよびキーファイルKFを別々に設けた場合を例示したが、例えば、図53に示すように、セキュアコンテナ104内において、コンテンツファイルCF内にキーファイルKFを格納するようにしてもよい。

この場合に、キーファイルKFを格納したコンテンツファイルCFに対して、コンテンツプロバイダ101の秘密鍵データK_{CP}，Sによる署名データが付される。

第1実施形態の第6変形例

上述した実施形態では、コンテンツデータCをコンテンツファイルCFに格納し、コンテンツ鍵データK_cおよび権利書データ106をキーファイルKF内に格納してコンテンツプロバイダ101からSAM105₁などに送信する場合を例示したが、コンテンツデータC、コンテンツ鍵データK_cおよび権利書データ106の少なくとも一つをファイル形式を採用せずにコンテンツプロバイダ101からSAM105₁などに、通信プロトコルに依存しない形式で送信してもよい。

【0314】

例えば、図54に示すように、コンテンツプロバイダ101において、コンテンツ鍵データK_cで暗号化されたコンテンツデータCと、暗号化されたコンテンツ鍵データK_cおよび暗号化された権利書データ106などを含むキーファイルKFとを格納したセキュアコンテナ104_sを作成し、セキュアコンテナ104_sをSAM105₁などに通信プロトコルに依存しない形式で送信してもよい。

【0315】

また、図55に示すように、コンテンツプロバイダ101からSAM105₁などに、コンテンツ鍵データK_cで暗号化されたコンテンツデータCと、暗号化

されたコンテンツ鍵データKcおよび暗号化された権利書データ106などを含むキーファイルKFとを通信プロトコルに依存しない形式で個別に送信してもよい。すなわち、コンテンツデータCをファイル形式にしないで、キーファイルKFと同一経路で送信する。

【0316】

また、図56に示すように、コンテンツプロバイダ101からSAM105₁などに、コンテンツ鍵データKcで暗号化されたコンテンツデータCを通信プロトコルに依存しない形式で送信すると共に、暗号化されたコンテンツ鍵データKcおよび暗号化された権利書データ106などを含むキーファイルKFをEMDサービスセンタ102からSAM105₁などに送信してもよい。すなわち、コンテンツデータCをファイル形式にしないで、キーファイルKFと別経路で送信する。

【0317】

また、図57に示すように、コンテンツプロバイダ101からSAM105₁などに、コンテンツ鍵データKcで暗号化されたコンテンツデータCと、コンテンツ鍵データKcおよび権利書データ106とを、通信プロトコルに依存しない形式で送信してもよい。すなわち、コンテンツデータC、コンテンツ鍵データKcおよび権利書データ106をファイル形式にしないで、同一経路で送信する。

【0318】

また、図58に示すように、コンテンツプロバイダ101からSAM105₁などに、コンテンツ鍵データKcで暗号化されたコンテンツデータCを、通信プロトコルに依存しない形式で送信すると共に、EMDサービスセンタ102からSAM105₁などにコンテンツ鍵データKcおよび権利書データ106を送信してもよい。すなわち、コンテンツデータC、コンテンツ鍵データKcおよび権利書データ106をファイル形式にしないで、別経路で送信する。

【0319】

第2実施形態

上述した実施形態では、コンテンツプロバイダ101からユーザホームネットワーク103のSAM105₁～105₄にコンテンツデータを直接配給する場

合を例示したが、本実施形態では、コンテンツプロバイダが提供するコンテンツデータを、サービスプロバイダを介してユーザホームネットワークのSAMに配給する場合について説明する。

【0320】

図59は、本実施形態のEMDシステム300の構成図である。

図59に示すように、EMDシステム300は、コンテンツプロバイダ301、EMDサービスセンタ302、ユーザホームネットワーク303、サービスプロバイダ310、ペイメントゲートウェイ90および決済機関91を有する。

コンテンツプロバイダ301、EMDサービスセンタ302、SAM305₁～305₄およびサービスプロバイダ310は、それぞれ請求項49および請求項59などに係わるデータ提供装置、管理装置、データ処理装置およびデータ配給装置に対応している。

コンテンツプロバイダ301は、サービスプロバイダ310に対してコンテンツデータを供給する点を除いて、前述した第1実施形態のコンテンツプロバイダ101と同じである。

また、EMDサービスセンタ302は、コンテンツプロバイダ101およびSAM505₁～505₄に加えて、サービスプロバイダ310に対しても認証機能、鍵データ管理機能および権利処理機能を有する点を除いて、前述した第1実施形態のEMDサービスセンタ102と同じである。

また、ユーザホームネットワーク303は、ネットワーク機器360₁およびAV機器360₂～360₄を有している。ネットワーク機器360₁はSAM305₁およびCAモジュール311を内蔵しており、AV機器360₂～360₄はそれぞれSAM305₂～305₄を内蔵している。

ここで、SAM305₁～305₄は、サービスプロバイダ310からセキュアコンテナ304の配給を受ける点と、コンテンツプロバイダ301に加えてサービスプロバイダ310についての署名データの検証処理およびSP用購入履歴データ（データ配給装置用購入履歴データ）309の作成を行なう点とを除いて、前述した第1実施形態のSAM105₁～105₄と同じである。

【0321】

先ず、EMDシステム300の概要について説明する。

EMDシステム300では、コンテンツプロバイダ301は、自らが提供しようとするコンテンツのコンテンツデータCの使用許諾条件などの権利内容を示す前述した第1実施形態と同様の権利書(UCP: Usage Control Policy)データ106およびコンテンツ鍵データKcを、高い信頼性のある権威機関であるEMDサービスセンタ302に送信する。権利書データ106およびコンテンツ鍵データKcは、EMDサービスセンタ302に登録されて権威化(認証)される。

【0322】

また、コンテンツプロバイダ301は、コンテンツ鍵データKcでコンテンツデータCを暗号化してコンテンツファイルCFを生成する。また、コンテンツプロバイダ301は、EMDサービスセンタ302から、各コンテンツファイルCFについて、それぞれ6か月分のキーファイルKFを受信する。

当該キーファイルKF内には、当該キーファイルKFの改竄の有無、当該キーファイルKFの作成者および送信者の正当性を検証するための署名データが格納されている。

そして、コンテンツプロバイダ301は、コンテンツファイルCF、キーファイルKFおよび自らの署名データとを格納した図5に示すセキュアコンテナ104を、インターネットなどのネットワーク、デジタル放送、記録媒体あるいは非公式なプロトコルを用いてあるいはオフラインなどでサービスプロバイダ310に供給する。

また、セキュアコンテナ104に格納された署名データは、対応するデータの改竄の有無、当該データの作成者および送信者の正当性を検証するために用いられる。

【0323】

サービスプロバイダ310は、コンテンツプロバイダ301からセキュアコンテナ104を受け取ると、署名データの検証を行なって、セキュアコンテナ104の作成者および送信者の確認する。

次に、サービスプロバイダ310は、例えばオフラインで通知されたコンテン

ツプロバイダ 301 が希望するコンテンツに対しての価格 (SRP) に、自らが
行ったオーサリングなどのサービスに対しての価格を加算した価格を示すプライ
スタグデータ (PT) 312 を作成する。

そして、サービスプロバイダ 310 は、セキュアコンテナ 104 から取り出し
たコンテンツファイル CF およびキーファイル KF と、プライスタグデータ 31
2 と、これらに対しての自らの秘密鍵データ $K_{SP, S}$ による署名データとを格
納したセキュアコンテナ 304 を作成する。

このとき、キーファイル KF は、配信用鍵データ $KD_1 \sim KD_6$ によって暗号
化されており、サービスプロバイダ 310 は当該配信用鍵データ $KD_1 \sim KD_6$
を保持していないため、サービスプロバイダ 310 はキーファイル KF の中身を見
たり、書き換えたりすることはできない。

また、EMD サービスセンタ 302 は、プライスタグデータ 312 を登録して
権威化する。

【0324】

サービスプロバイダ 310 は、オンラインおよび／またはオフラインでセキュ
アコンテナ 304 をユーザホームネットワーク 303 に配給する。

このとき、オフラインの場合には、セキュアコンテナ 304 は ROM 型の記録
媒体などに記録されて $SAM305_1 \sim 305_4$ にそのまま供給される。一方、
オンラインの場合には、サービスプロバイダ 310 と CA モジュール 311 との
間で相互認証を行い、セキュアコンテナ 304 をサービスプロバイダ 310 にお
いてセッション鍵データ K_{SES} を用いた暗号化して送信し、CA モジュール 3
11 において受信したセキュアコンテナ 304 をセッション鍵データ K_{SES} を
用いて復号した後に、 $SAM305_1 \sim 305_4$ に転送する。

この場合に、コンテンツプロバイダ 301 からユーザホームネットワーク 30
3 にセキュアコンテナ 304 を送信する通信プロトコルとして、デジタル放送で
あれば MHEG (Multimedia and Hypermedia in
formation coding Experts Group) プロトコル
が用いられ、インターネットであれば XML/SMIL/HTML (Hyper
Text Markup Language) が用いられ、これらの通信プロト

コル内に、セキュアコンテナ 304 が、当該通信プロトコル（符号化方式など）に依存しない形式でトンネリングして埋め込まれる。

従って、通信プロトコルとセキュアコンテナ 304 との間でフォーマットの整合性をとる必要性はなく、セキュアコンテナ 304 のフォーマットを柔軟に設定できる。

【0325】

次に、SAM305₁～305₄において、セキュアコンテナ 304 内に格納された署名データを検証して、セキュアコンテナ 304 に格納されたコンテンツファイル CF およびキーファイル KF の作成者および送信者の正当性を確認する。そして、SAM305₁～305₄において、当該正当性が確認されると、EMD サービスセンタ 302 から配給された対応する期間の配信用鍵データ KD₁～KD₃を用いてキーファイル KF を復号する。

SAM305₁～305₄に供給されたセキュアコンテナ 304 は、ネットワーク機器 360₁ および AV 機器 360₂～360₄において、ユーザの操作に応じて購入・利用形態が決定された後に、再生や記録媒体への記録などの対象となる。

SAM305₁～305₄は、上述したセキュアコンテナ 304 の購入・利用の履歴を利用履歴（Usage Log）データ 308 として記録する。

利用履歴データ（履歴データまたは管理装置用履歴データ）308 は、例えば、EMD サービスセンタ 302 からの要求に応じて、ユーザホームネットワーク 303 から EMD サービスセンタ 302 に送信される。

また、SAM305₁～305₄は、コンテンツの購入形態が決定されると、当該購入形態を示す利用制御状態データ（UCS: Usage control state Data）166 を EMD サービスセンタ 302 に送信する。

【0326】

EMD サービスセンタ 302 は、利用履歴データ 308 に基づいて、コンテンツプロバイダ 301 およびサービスプロバイダ 310 の各々について、課金内容を決定（計算）し、その結果に基づいて、ペイメントゲートウェイ 90 を介して銀行などの決済機関 91 に決済を行なう。これにより、ユーザホームネットワー

ク 103 のユーザが支払った金銭が、EMD サービスセンタ 102 による決済処理によって、コンテンツプロバイダ 101 およびサービスプロバイダ 310 に分配される。

【0327】

本実施形態では、EMD サービスセンタ 302 は、認証機能、鍵データ管理機能および権利処理（利益分配）機能を有している。

すなわち、EMD サービスセンタ 302 は、中立の立場にある最高の権威機関であるルート認証局 92 に対してのセカンド認証局（Second Certificate Authority）としての役割を果たし、コンテンツプロバイダ 301、サービスプロバイダ 310 および SAM305₁～305₄において署名データの検証処理に用いられる公開鍵データの公開鍵証明書データに、EMD サービスセンタ 302 の秘密鍵データによる署名を付けることで、当該公開鍵データの正当性を認証する。また、前述したように、コンテンツプロバイダ 301 の権利書データ 106、コンテンツ鍵データ Kc およびサービスプロバイダ 310 のプライスタグデータ 312 を登録して権威化することも、EMD サービスセンタ 302 の認証機能によるものである。

また、EMD サービスセンタ 302 は、例えば、配信用鍵データ KD₁～KD₆などの鍵データの管理を行なう鍵データ管理機能を有する。

また、EMD サービスセンタ 302 は、コンテンツプロバイダ 301 が登録した権利書データ 106 と SAM305₁～SAM305₄ から入力した利用履歴データ 308 とサービスプロバイダ 310 が登録したプライスタグデータ 312 とに基づいて、ユーザホームネットワーク 303 のユーザによるコンテンツの購入・利用に対して決済を行い、ユーザが支払った金銭をコンテンツプロバイダ 301 およびサービスプロバイダ 310 に分配して支払う権利処理（利益分配）機能を有する。

【0328】

以下、コンテンツプロバイダ 301 の各構成要素について詳細に説明する。

〔コンテンツプロバイダ 301〕

図 60 は、コンテンツプロバイダ 301 の機能ブロック図であり、サービスプ

ロバイダ 310 との間で送受信されるデータに関連するデータの流れが示されている。

図 60 に示すように、コンテンツプロバイダ 301 は、コンテンツマスターデータベース 111、電子透かし情報付加部 112、圧縮部 113、暗号化部 114、乱数発生部 115、署名処理部 117、セキュアコンテナ作成部 118、セキュアコンテナデータベース 118a、キーファイルデータベース 118b、記憶部 119、相互認証部 120、暗号化・復号部 121、権利書データ作成部 122、EMD サービスセンタ管理部 125 および サービスプロバイダ管理部 324 を有する。

【0329】

図 60 において、図 3 と同一符号を付した構成要素は、前述した第 1 実施形態において図 3 および図 4 を参照しながら説明した同一符号の構成要素と同じである。

すなわち、コンテンツプロバイダ 301 は、図 3 に示す SAM 管理部 124 の代わりに サービスプロバイダ管理部 324 を設けた構成をしている。

サービスプロバイダ管理部 324 は、セキュアコンテナ作成部 118 から入力した図 5 に示すセキュアコンテナ 104 を、オフラインおよび／またはオンラインで、図 59 に示す サービスプロバイダ 310 に提供する。

【0330】

サービスプロバイダ管理部 324 は、図 5 に示すセキュアコンテナ 104 をオンラインで サービスプロバイダ 310 に配信する場合には、暗号化・復号部 121 においてセッション鍵データ K_{SES} を用いてセキュアコンテナ 104 を暗号化した後に、ネットワークを介して サービスプロバイダ 310 に配信する。

【0331】

また、図 4 に示すしたコンテンツプロバイダ 101 内でのデータの流れは、コンテンツプロバイダ 301 にも同様に適用される。

【0332】

以下、コンテンツプロバイダ 301 から サービスプロバイダ 310 にセキュアコンテナ 104 を送信する際の処理の流れを説明する。

図 6 1 および図 6 2 は、コンテンツプロバイダ 3 0 1 からサービスプロバイダ 3 1 0 にセキュアコンテナ 1 0 4 を送信する際の処理の流れを示すフローチャートである。

ステップ C 1 : コンテンツプロバイダ 3 0 1 とサービスプロバイダ 3 1 0 との間で相互認証を行う。

ステップ C 2 : ステップ C 1 の相互認証によって得られたセッション鍵データ K_{SES} を、コンテンツプロバイダ 3 0 1 およびサービスプロバイダ 3 1 0 の間で共有する。

ステップ C 3 : サービスプロバイダ 3 1 0 によって、コンテンツプロバイダ 3 0 1 が所有する (C P 用) セキュアコンテナデータベース 1 1 8 a にアクセスが行われる。

ステップ C 4 : サービスプロバイダ 3 1 0 は、例えば、セキュアコンテナデータベース 1 1 8 a において一元的に管理されているコンテンツ ID とメタデータとのリストを参照して自らの配信サービスに必要なセキュアコンテナ 1 0 4 を選択する。

【 0 3 3 3 】

ステップ C 5 : コンテンツプロバイダ 3 0 1 は、ステップ C 4 で選択したセキュアコンテナ 1 0 4 を、ステップ C 2 で共有したセッション鍵データ K_{SES} を用いて暗号化する。

ステップ C 6 : コンテンツプロバイダ 3 0 1 は、ステップ C 5 で得られたセキュアコンテナ 1 0 4 を、コンテンツプロバイダ用商品配送プロトコルに挿入する。

【 0 3 3 4 】

ステップ C 7 : サービスプロバイダ 3 1 0 は、ダウンロードを行う。

ステップ C 8 : サービスプロバイダ 3 1 0 は、コンテンツプロバイダ用商品配送プロトコルからセキュアコンテナ 1 0 4 を取り出す。

ステップ C 9 : サービスプロバイダ 3 1 0 は、セキュアコンテナ 1 0 4 を、ステップ C 2 で共有したセッション鍵データ K_{SES} を用いて復号する。

ステップ C 1 0 : サービスプロバイダ 3 1 0 は、復号したセキュアコンテナ 1

04に格納されている署名データを検証して、送信者の正当性を確認し、送信者が正当であることの確認を条件にステップC11の処理を行う。

ステップC11：サービスプロバイダ310は、セキュアコンテナ104を自らのセキュアコンテナデータベースに格納する。

【0335】

〔サービスプロバイダ310〕

サービスプロバイダ310は、コンテンツプロバイダ301から提供を受けたセキュアコンテナ104内のコンテンツファイルCFおよびキーファイルKFと、自らが生成したプライスタグデータ312とを格納したセキュアコンテナ304を作成し、ユーザホームネットワーク303のネットワーク機器360₁およびAV機器360₂～360₄にセキュアコンテナ304をオンラインおよび／またはオフラインで配給する。

サービスプロバイダ310によるコンテンツ配給のサービス形態には、大きく分けて、独立型サービスと連動型サービスとがある。

独立型サービスは、例えば、コンテンツを個別に配給するダウンロード専用のサービスである。また、連動型サービスは、番組、CM（広告）に連動してコンテンツを配給するサービスであり、例えば、ドラマ番組のストリーム内にドラマの主題歌や挿入歌のコンテンツが格納してある。ユーザは、ドラマ番組を見ているときに、そのストリーム中にある主題歌や挿入歌のコンテンツを購入できる。

【0336】

図63は、サービスプロバイダ310の機能ブロック図である。

なお、図63には、コンテンツプロバイダ301から供給を受けたセキュアコンテナ104を用いて作成したセキュアコンテナ304をユーザホームネットワーク303に供給する際のデータの流れが示されている。

図63に示すように、サービスプロバイダ310は、コンテンツプロバイダ管理部350、記憶部351、相互認証部352、暗号化・復号部353、署名処理部354、セキュアコンテナ作成部355、セキュアコンテナデータベース355a、プライスタグデータ作成部356、ユーザホームネットワーク管理部357、EMDサービスセンタ管理部358およびユーザ嗜好フィルタ生成部92

0を有する。

【0337】

以下、コンテンツプロバイダ301から供給を受けたセキュアコンテナ104からセキュアコンテナ304を作成し、これをユーザホームネットワーク303に配給する際のサービスプロバイダ310内での処理の流れを図63および図64を参照しながら説明する。

図64は、コンテンツプロバイダ301からユーザホームネットワーク303にセキュアコンテナ304を配給する処理を説明するためのフローチャートである。

<ステップD1>

コンテンツプロバイダ管理部350は、オンラインおよび／またはオフラインで、コンテンツプロバイダ301から図5に示すセキュアコンテナ104の供給を受けてセキュアコンテナ104を記憶部351に書き込む。

このとき、コンテンツプロバイダ管理部350は、オンラインの場合には、図60に示す相互認証部120と図63に示す相互認証部352との間の相互認証によって得られたセッション鍵データ K_{SES} を用いて、セキュアコンテナ104を暗号化・復号部353において復号した後に、記憶部351に書き込む。

なお、サービスプロバイダ310は、記憶部351とは別に、セキュアコンテナ104を格納するための専用のセキュアコンテナデータベースを有してもよい。

【0338】

<ステップD2>

次に、署名処理部354において、記憶部351に記憶されているセキュアコンテナ104の図5(C)に示す署名データ SIG_1 , ESC を記憶部351から読み出したEMDサービスセンタ302の公開鍵データ $K_{ESC, P}$ を用いて検証し、その正当性が認められた後に、図5(C)に示す公開鍵証明書データ CER_{CP} から公開鍵データ $K_{CP, P}$ を取り出す。

次に、署名処理部354は、当該取り出した公開鍵データ $K_{CP, P}$ を用いて、記憶部351に記憶されているセキュアコンテナ104の図5(A), (B)

に示す署名データ SIG_6, CP , SIG_7, CP の検証、すなわちコンテンツファイル CF の作成者および送信者と、キーファイル KF の送信者との正当性の検証を行う。

また、署名処理部 354 は、記憶部 351 から読み出した公開鍵データ $K_{ESC, P}$ を用いて、図 5 (B) に示すキーファイル KF に格納された署名データ $SIG_{K1, ESC}$ の検証、すなわちキーファイル KF の作成者の正当性の検証を行う。このとき、署名データ $SIG_{K1, ESC}$ の検証は、キーファイル KF が EMD サービスセンタ 302 に登録されているか否かの検証も兼ねている。

【0339】

<ステップ D3>

次に、セキュアコンテナ作成部 355 は、署名データ SIG_6, CP , SIG_7, CP , $SIG_{K1, ESC}$ の正当性が確認されると、記憶部 351 からコンテンツファイル CF およびその署名データ SIG_6, CP と、キーファイル KF およびその署名データ SIG_7, CP と、サービスプロバイダ 310 の公開鍵証明書データ CER_{SP} およびその署名データ $SIG_{61, ESC}$ と、コンテンツプロバイダ 301 の公開鍵証明書データ CER_{CP} およびその署名データ $SIG_{1, ESC}$ とを読み出す。

【0340】

また、プライスタグデータ作成部 356 は、例えばコンテンツプロバイダ 301 からオフラインで通知されたコンテンツプロバイダ 301 が要求するコンテンツに対しての価格に、自らのサービスの価格を加算した価格を示すプライスタグデータ 312 を作成し、記憶部 351 に記憶する。

【0341】

また、署名処理部 354 は、コンテンツファイル CF 、キーファイル KF およびプライスタグデータ 312 のハッシュ値をとり、サービスプロバイダ 310 の秘密鍵データ $K_{SP, P}$ を用いて、署名データ $SIG_{62, SP}$, $SIG_{63, SP}$, $SIG_{64, SP}$ を作成し、これをセキュアコンテナ作成部 355 に出力する。

ここで、署名データ $SIG_{62, SP}$ はコンテンツファイル CF の送信者の正

当性を検証するために用いられ、署名データ SIG₆₃, SP はキーファイル KF の送信者の正当性を検証するために用いられ、署名データ SIG₆₄, SP はプライスタグデータ 312 の作成者および送信者の正当性を検証するために用いられる。

【0342】

次に、セキュアコンテナ作成部 355 は、図 65 (A) ~ (D) に示すように、コンテンツファイル CF およびその署名データ SIG₆, CP, SIG₆₂, SP と、キーファイル KF およびその署名データ SIG₇, CP, SIG₆₃, ESC と、プライスタグデータ 312 およびその署名データ SIG₆₄, SP と、公開鍵証明書データ CER_{SP} およびその署名データ SIG₆₁, ESC と、公開鍵証明書データ CER_{CP} およびその署名データ SIG₁, ESC とを格納したセキュアコンテナ 304 を作成し、セキュアコンテナデータベース 355a に格納する。

セキュアコンテナデータベース 355a に格納されたセキュアコンテナ 304 は、例えば、コンテンツ ID などを用いてサービスプロバイダ 310 によって一元的に管理される。

【0343】

<ステップ D4>

セキュアコンテナ作成部 355 は、ユーザホームネットワーク 303 からの要求に応じたセキュアコンテナ 304 をセキュアコンテナデータベース 355a から読み出してユーザホームネットワーク管理部 357 に出力する。

このとき、セキュアコンテナ 304 は、複数のコンテンツファイル CF と、それらにそれぞれ対応した複数のキーファイル KF とを格納した複合コンテナであってもよい。例えば、単数のセキュアコンテナ 304 内に、それぞれ曲、ビデオクリップ、歌詞カード、ライナーノーツおよびジャケットに関する複数のコンテンツファイル CF を単数のセキュアコンテナ 304 に格納してもよい。これらの複数のコンテンツファイル CF などは、ディレクトリー構造でセキュアコンテナ 304 内に格納してもよい。

【0344】

また、セキュアコンテナ304は、デジタル放送で送信される場合には、MHEG (Multimedia and Hypermedia information coding Experts Group) プロトコルが用いられ、インターネットで送信される場合にはXML/SMIL/HTML (Hyper Text Markup Language) プロトコルが用いられる。

このとき、セキュアコンテナ304内のコンテンツファイルCFおよびキーファイルKFなどは、MHEGおよびHTMLのプロトコルをトンネリングした符号化方式に依存しない形式で、サービスプロバイダ310とユーザホームネットワーク303との間で採用される通信プロトコル内の所定の階層に格納される。

【0345】

例えば、セキュアコンテナ304をデジタル放送で送信する場合には、図66に示すように、コンテンツファイルCFが、MHEGオブジェクト (Object) 内のMHEGコンテンツデータとして格納される。

また、MHEGオブジェクトは、トランスポート層プロトコルにおいて、動画である場合にはPES (Packetized Elementary Stream) - Videoに格納され、音声である場合にはPES - Audioに格納され、静止画である場合にはPrivate - Dataに格納される。

また、図67に示すように、キーファイルKF、プライスタグデータ312および公開鍵証明書データ CER_{CP} 、 CER_{SP} は、トランスポート層プロトコルのTS Packet 内のECM (Entitlement Control Message) に格納される。

ここで、コンテンツファイルCF、キーファイルKF、プライスタグデータ312および公開鍵証明書データ CER_{CP} 、 CER_{SP} は、コンテンツファイルCFのヘッダ内のディレクトリ構造データ DSD_1 によって相互間のリンクが確立されている。

【0346】

次に、ユーザホームネットワーク管理部357は、セキュアコンテナ304を、オフラインおよび／またはオンラインでユーザホームネットワーク303に供給する。

ユーザホームネットワーク管理部357は、セキュアコンテナ304をオンラインでユーザホームネットワーク303のネットワーク機器360₁に配信する場合には、相互認証後に、暗号化・復号部352においてセッション鍵データ K_{SES} を用いてセキュアコンテナ304を暗号化した後に、ネットワークを介してネットワーク機器360₁に配信する。

【0347】

なお、ユーザホームネットワーク管理部357は、セキュアコンテナ304を例えば衛星などを介して放送する場合には、セキュアコンテナ304をスクランブル鍵データ K_{SCR} を用いて暗号化する。また、スクランブル鍵データ K_{SCR} をワーク鍵データ K_W を暗号化し、ワーク鍵データ K_W をマスタ鍵データ K_M を用いて暗号化する。

そして、ユーザホームネットワーク管理部357は、セキュアコンテナ304と共に、スクランブル鍵データ K_{SCR} およびワーク鍵データ K_W を、衛星を介してユーザホームネットワーク303に送信する。

また、例えば、マスタ鍵データ K_M を、ICカードなどに記憶してオフラインでユーザホームネットワーク303に配給する。

【0348】

また、ユーザホームネットワーク管理部357は、ユーザホームネットワーク303から、当該サービスプロバイダ310が配給したコンテンツデータCに関するSP用購入履歴データ309を受信すると、これを記憶部351に書き込む。

サービスプロバイダ310は、将来のサービス内容を決定する際に、SP用購入履歴データ309を参照する。また、ユーザ嗜好フィルタ生成部920は、SP用購入履歴データ309に基づいて、当該SP用購入履歴データ309を送信したSAM305₁～305₄のユーザの嗜好を分析してユーザ嗜好フィルタデータ900を生成し、これをユーザホームネットワーク管理部357を介してユーザホームネットワーク303のCAモジュール311に送信する。

【0349】

図68には、サービスプロバイダ310内におけるEMDサービスセンタ30

2 との間の通信に関連するデータの流れが示されている。

なお、以下に示す処理を行う前提として、サービスプロバイダ 310 の関係者は、例えば、自らの身分証明書および決済処理を行う銀行口座などを用いて、オフラインで、EMD サービスセンタ 302 に登録処理を行い、グローバルユニークな識別子 SP_ID を得ている。識別子 SP_ID は、記憶部 351 に記憶される。

【0350】

まず、サービスプロバイダ 310 が、EMD サービスセンタ 302 に、自らの秘密鍵データ $K_{SP, S}$ に対応する公開鍵データ $K_{SP, S}$ の正当性を証明する公開鍵証明書データ CER_{SP} を要求する場合の処理を図 68 を参照しながら説明する。

サービスプロバイダ 310 は、真性乱数発生器を用いて乱数を発生して秘密鍵データ $K_{SP, S}$ を生成し、当該秘密鍵データ $K_{SP, S}$ に対応する公開鍵データ $K_{SP, P}$ を作成して記憶部 351 に記憶する。

EMD サービスセンタ管理部 358、サービスプロバイダ 310 の識別子 SP_ID および公開鍵データ $K_{SP, P}$ を記憶部 351 から読み出す。

そして、EMD サービスセンタ管理部 358 は、識別子 SP_ID および公開鍵データ $K_{SP, P}$ を、EMD サービスセンタ 302 に送信する。

そして、EMD サービスセンタ管理部 348 は、当該登録に応じて、公開鍵証明書データ CER_{SP} およびその署名データ $SIG_{61, ESC}$ を EMD サービスセンタ 302 から入力して記憶部 351 に書き込む。

【0351】

次に、サービスプロバイダ 310 が、EMD サービスセンタ 302 にプライスタグデータ 312 を登録して権威化する場合の処理を図 68 を参照して説明する。

【0352】

この場合には、署名処理部 354 において、記憶部 351 から読み出したプライスタグデータ 312 およびグローバルユニークな識別子であるコンテンツ ID を格納した図 69 に示すモジュール Mod_{103} のハッシュ値が求められ、秘密

鍵データ $K_{SP, S}$ を用いて署名データ $SIG_{80, SP}$ が生成される。

また、記憶部 351 から公開鍵証明書データ CER_{SP} およびその署名データ $SIG_{61, ESC}$ が読み出される。

そして、図 69 に示すプライスタグ登録要求用モジュール Mod_{102} が、相互認証部 352 と EMD サービスセンタ 302 との間の相互認証によって得られたセッション鍵データ K_{SES} を用いて暗号化・復号部 353 において暗号化された後に、EMD サービスセンタ管理部 358 から EMD サービスセンタ 302 に送信される。

なお、モジュール Mod_{102} に、サービスプロバイダ 310 のグローバルユニークな識別子 SP_ID を格納してもよい。

【0353】

また、EMD サービスセンタ管理部 358 は、EMD サービスセンタ 302 から受信した決済レポートデータ 307s を記憶部 351 に書き込む。

【0354】

また、EMD サービスセンタ管理部 358 は、EMD サービスセンタ 302 から受信したマーケティング情報データ 904 を記憶部 351 に記憶する。

マーケティング情報データ 904 は、サービスプロバイダ 310 が今後配給するコンテンツデータ C を決定する際に参考にされる。

【0355】

〔EMD サービスセンタ 302〕

EMD サービスセンタ 302 は、前述したように、認証局 (CA: Certificate Authority)、鍵管理 (Key Management) 局および権利処理 (Rights Clearing) 局としての役割を果たす。

図 70 は、EMD サービスセンタ 302 の機能の構成図である。

図 70 に示すように、EMD サービスセンタ 302 は、鍵サーバ 141、鍵データベース 141a、KF 作成部 153、決済処理部 442、署名処理部 443、決算機関管理部 144、証明書・権利書管理部 445、権利書データベース 445a、証明書データベース 445b、コンテンツプロバイダ管理部 148、C

Pデータベース148a、SAM管理部149、SAMデータベース149a、相互認証部150、暗号化・復号部151、サービスプロバイダ管理部390、SPデータベース390a、コンテンツID作成部851、ユーザ嗜好フィルタ生成部901およびマーケティング情報データ生成部902を有する。

図70において、図23および図24と同じ符号を付した機能ブロックは、第1実施形態で説明した同一符号の機能ブロックと略同じ機能を有している。

【0356】

以下、図70において、新たな符号を付した機能ブロックについて説明する。

なお、図70には、EMDサービスセンタ302内の機能ブロック相互間のデータの流れのうち、サービスプロバイダ310との間で送受信されるデータに関連するデータの流れが示されている。

また、図71には、EMDサービスセンタ302内の機能ブロック相互間のデータの流れのうち、コンテンツプロバイダ301との間で送受信されるデータに関連するデータの流れが示されている。

また、図72には、EMDサービスセンタ302内の機能ブロック相互間のデータの流れのうち、図59に示すSAM305₁～305₄および決済機関91との間で送受信されるデータに関連するデータの流れが示されている。

【0357】

決算処理部442は、図72に示すように、SAM305₁～305₄から入力した利用履歴データ308と、証明書・権利書管理部445から入力した標準小売価格データSRPおよびプライスタグデータ312に基づいて決済処理を行う。なお、この際に、決済処理部442は、サービスプロバイダ310によるダンプの有无などを監視する。

決済処理部442は、決済処理により、図72に示すように、コンテンツプロバイダ301についての決済レポートデータ307cおよび決済請求権データ152cを作成し、これらをそれぞれコンテンツプロバイダ管理部148および決算機関管理部144に出力する。

また、決済処理により、図70および図72に示すように、サービスプロバイダ310についての決済レポートデータ307sおよび決済請求権データ152

s を作成し、これらをそれぞれサービスプロバイダ管理部 390 および決算機関管理部 144 に出力する。

ここで、決済請求権データ 152 c, 152 s は、当該データに基づいて、決済機関 91 に金銭の支払いを請求できる権威化されたデータである。

【0358】

ここで、利用履歴データ 308 は、第 1 実施形態で説明した利用履歴データ 108 と同様に、セキュアコンテナ 304 に関連したライセンス料の支払いを決定する際に用いられる。利用履歴データ 308 には、例えば、図 73 に示すように、セキュアコンテナ 304 に格納されたコンテンツデータ C の識別子であるコンテンツ ID、セキュアコンテナ 304 に格納されたコンテンツデータ C を提供したコンテンツプロバイダ 301 の識別子 CP_ID、セキュアコンテナ 304 を配給したサービスプロバイダ 310 の識別子 SP_ID、コンテンツデータ C の信号諸元データ、セキュアコンテナ 304 内のコンテンツデータ C の圧縮方法、セキュアコンテナ 304 を記録した記録媒体の識別子 Media_ID、セキュアコンテナ 304 を配給を受けた SAM305₁ ~ 305₄ の識別子 SAM_ID、当該 SAM105₁ ~ 105₄ のユーザの USER_ID などが記述されている。従って、EMD サービスセンタ 302 は、コンテンツプロバイダ 301 およびサービスプロバイダ 310 の所有者以外にも、例えば、圧縮方法や記録媒体などのライセンス所有者に、ユーザホームネットワーク 303 のユーザが支払った金銭を分配する必要がある場合には、予め決められた分配率表に基づいて各相手に支払う金額を決定し、当該決定に応じた決済レポートデータおよび決済請求権データを作成する。

【0359】

証明書・権利書管理部 445 は、証明書データベース 445 b に登録されて権威化された公開鍵証明書データ CER_{CP}、公開鍵証明書データ CER_{SP} および公開鍵証明書データ CER_{SAM1} ~ CER_{SAM2} などを読み出すと共に、権利書データベース 445 a にコンテンツプロバイダ 301 の権利書データ 106 およびコンテンツ鍵データ Kc、並びにサービスプロバイダ 310 のプライスタグデータ 312などを登録して権威化する。

このとき、証明書・権利書管理部 445 は、権利書データ 106、コンテンツ鍵データ K_c およびプライスタグデータ 312 などのハッシュ値をとり、秘密鍵データ $K_{ESC, S}$ を用いた署名データを付して権威化証明書データを作成する。

【0360】

コンテンツプロバイダ管理部 148 は、コンテンツプロバイダ 101 との間で通信する機能を有し、登録されているコンテンツプロバイダ 101 の識別子 CP_ID などを管理する CP データベース 148a にアクセスできる。

【0361】

ユーザ嗜好フィルタ生成部 901 は、利用履歴データ 308 に基づいて、当該利用履歴データ 308 を送信した $SAM305_1 \sim 305_4$ のユーザの嗜好に応じたコンテンツデータ C を選択するためのユーザ嗜好フィルタデータ 903 を生成し、ユーザ嗜好フィルタデータ 903 を SAM 管理部 149 を介して、当該利用履歴データ 308 を送信した $SAM305_1 \sim 305_4$ に送信する。

【0362】

マーケティング情報データ生成部 902 は、利用履歴データ 308 に基づいて、例えば、複数のサービスプロバイダ 310 によってユーザホームネットワーク 103 に配給されたコンテンツデータ C の全体の購入状況などを示すマーケティング情報データ 904 を生成し、これをサービスプロバイダ管理部 390 を介して、サービスプロバイダ 310 に送信する。サービスプロバイダ 310 は、マーケティング情報データ 904 を参考にして、今後提供するサービスの内容を決定する。

【0363】

以下、EMD サービスセンタ 302 内での処理の流れを説明する。

EMD サービスセンタ 302 から $SAM305_1 \sim 305_4$ への配信用鍵データ $KD_1 \sim KD_3$ の送信は、第 1 実施形態の場合と同様に行なわれる。

【0364】

また、EMD サービスセンタ 302 がコンテンツプロバイダ 301 から、公開鍵証明書データの発行要求を受けた場合の処理は証明書・権利書管理部 445 が

証明書データベース 445b にアクセスする点を除いて、前述した第 1 実施形態と同じである。また、権利書データ 106 などを登録する処理も、証明書・権利書管理部 445 が権利書データベース 445a に当該データを格納する点を除いて前述した第 1 実施形態の場合と同様である。

【0365】

次に、EMD サービスセンタ 302 がサービスプロバイダ 310 から、公開鍵証明書データの発行要求を受けた場合の処理を、図 70 を参照しながら説明する。

この場合に、サービスプロバイダ管理部 390 は、予め EMD サービスセンタ 302 によって与えられたサービスプロバイダ 310 の識別子 SP_ID 、公開鍵データ $K_{SP, P}$ および署名データ $SIG_{70, SP}$ をサービスプロバイダ 310 から受信すると、これらを、相互認証部 150 と図 63 に示す相互認証部 352 と間の相互認証で得られたセッション鍵データ K_{SES} を用いて復号する。

そして、当該復号した署名データ $SIG_{70, SP}$ の正当性を署名処理部 443 において確認した後に、識別子 SP_ID および公開鍵データ $K_{SP, P}$ に基づいて、当該公開鍵証明書データの発行要求を出したサービスプロバイダ 310 が SP データベース 390a に登録されているか否かを確認する。

そして、証明書・権利書管理部 445 は、当該サービスプロバイダ 310 の公開鍵証明書データ CER_{SP} を証明書データベース 445b から読み出してサービスプロバイダ管理部 390 に出力する。

また、署名処理部 443 は、公開鍵証明書データ CER_{SP} のハッシュ値を取り、EMD サービスセンタ 302 の秘密鍵データ $K_{ESC, S}$ を用いて、署名データ $SIG_{61, ESC}$ を作成し、これをサービスプロバイダ管理部 390 に出力する。

そして、サービスプロバイダ管理部 390 は、公開鍵証明書データ CER_{SP} およびその署名データ $SIG_{61, ESC}$ を、相互認証部 150 と図 63 に示す相互認証部 352 と間の相互認証で得られたセッション鍵データ K_{SES} を用いて暗号化した後に、サービスプロバイダ 310 に送信する。

【0366】

なお、EMDサービスセンタ302がSAM105₁～105₄から、公開鍵証明書データの発行要求を受けた場合の処理は、第1実施形態と同様である。

また、EMDサービスセンタ302が、コンテンツプロバイダ301から権利書データ106およびコンテンツ鍵データK_cの登録要求を受けた場合の処理も、第1実施形態と同様である。

また、EMDサービスセンタ302が、コンテンツプロバイダ301から受信した登録用モジュールMod₂に応じてキーファイルKFを作成してコンテンツプロバイダ301に送信する処理も、第1実施形態と同様である。

【0367】

次に、EMDサービスセンタ302が、サービスプロバイダ310からプライスタグデータ312の登録要求を受けた場合の処理を、図70を参照しながら説明する。

この場合には、サービスプロバイダ管理部390がサービスプロバイダ310から図69に示すプライスタグ登録要求モジュールMod₁₀₂を受信すると、相互認証部150と図63に示す相互認証部352と間の相互認証で得られたセッション鍵データK_{SES}を用いてプライスタグ登録要求モジュールMod₁₀₂を復号する。

そして、当該復号したプライスタグ登録要求モジュールMod₁₀₂に格納された署名データSIG₈₀, S_Pの正当性を署名処理部443において確認した後、プライスタグ登録要求モジュールMod₁₀₂に格納されたプライスタグデータ312を、証明書・権利書管理部445を介して権利書データベース445aに登録して権威化する。

【0368】

次に、EMDサービスセンタ302において決済を行なう場合の処理を図72を参照しながら説明する。

SAM管理部149は、ユーザホームネットワーク303の例えばSAM305₁から利用履歴データ308およびその署名データSIG₂₀₅, SAM₁を入力すると、利用履歴データ308および署名データSIG₂₀₅, SAM₁を、相互認証部150とSAM305₁～305₄との間の相互認証によって得ら

れたセッション鍵データ K_{SES} を用いて復号し、 $SAM305_1$ の公開鍵データ $K_{SAM1, p}$ を用いて署名データ SIG_{205} 、 $SAM1$ の検証を行なった後に、決算処理部442に出力する。

【0369】

そして、決済処理部442は、 $SAM305_1$ から入力した利用履歴データ308と、証明書・権利書管理部445から入力した標準小売価格データSRPおよびプライスタグデータ312とに基づいて決済処理を行う。

決済処理部442は、決済処理により、図72に示すように、コンテンツプロバイダ301についての決済レポートデータ307cおよび決済請求権データ152cを作成し、これらをそれぞれコンテンツプロバイダ管理部148および決算機関管理部144に出力する。

また、決済処理により、図70および図72に示すように、サービスプロバイダ310についての決済レポートデータ307sおよび決済請求権データ152sを作成し、これらをそれぞれサービスプロバイダ管理部390および決算機関管理部144に出力する。

【0370】

次に、決算機関管理部144は、決済請求権データ152c、152sと、それらについて秘密鍵データ $K_{SEC, S}$ を用いて作成した署名データとを、相互認証およびセッション鍵データ K_{SES} による復号を行なった後に、図59に示すペイメントゲートウェイ90を介して決済機関91に送信する。

これにより、決済請求権データ152cに示される金額の金銭がコンテンツプロバイダ301に支払われ、決済請求権データ152sに示される金額の金銭がサービスプロバイダ310に支払われる。

【0371】

次に、EMDサービスセンタ302がコンテンツプロバイダ301およびサービスプロバイダ310に決済レポートデータ307cおよび307sを送信する場合の処理を説明する。

決算処理部442において決済が行なわれると、決算処理部442からコンテンツプロバイダ管理部148に決済レポートデータ307cが出力される。

コンテンツプロバイダ管理部 148 は、決算処理部 442 から決済レポートデータ 307c を入力すると、これを、相互認証部 150 と図 60 に示す相互認証部 120 と間の相互認証で得られたセッション鍵データ K_{SES} を用いて暗号化した後に、コンテンツプロバイダ 301 に送信する。

また、決算処理部 442 において決済が行なわれると、決算処理部 442 からサービスプロバイダ管理部 390 に決済レポートデータ 307s が出力される。

サービスプロバイダ管理部 390 は、決算処理部 442 から決済レポートデータ 307s を入力すると、これを、相互認証部 150 と図 63 に示す相互認証部 352 と間の相互認証で得られたセッション鍵データ K_{SES} を用いて暗号化した後に、サービスプロバイダ 310 に送信する。

【0372】

EMD サービスセンタ 302 は、その他に、第 1 実施形態の EMD サービスセンタ 102 と同様に、SAM 305₁ ~ 305₄ の出荷時の処理と、SAM 登録リストの登録処理とを行なう。

【0373】

〔ユーザホームネットワーク 303〕

ユーザホームネットワーク 303 は、図 59 に示すように、ネットワーク機器 360₁ および A/V 機器 360₂ ~ 360₄ を有している。

ネットワーク機器 360₁ は、CA モジュール 311 および SAM 305₁ を内蔵している。また、A/V 機器 360₂ ~ 360₄ は、それぞれ SAM 305₂ ~ 305₄ を内蔵している。

SAM 305₁ ~ 305₄ の相互間は、例えば、1394 シリアルインタフェースバスなどのバス 191 を介して接続されている。

なお、A/V 機器 360₂ ~ 360₄ は、ネットワーク通信機能を有していてもよいし、ネットワーク通信機能を有しておらず、バス 191 を介してネットワーク機器 360₁ のネットワーク通信機能を利用してもよい。

また、ユーザホームネットワーク 303 は、ネットワーク機能を有していない A/V 機器のみを有していてもよい。

【0374】

以下、ネットワーク機器 360₁ について説明する。

図 74 は、ネットワーク機器 360₁ の構成図である。

図 74 に示すように、ネットワーク機器 360₁ は、通信モジュール 162、CAモジュール 311、復号モジュール 905、SAM305₁、復号・伸長モジュール 163、購入・利用形態決定操作部 165、ダウンロードメモリ 167、再生モジュール 169 および外部メモリ 201 を有する。

図 74 において、図 25 と同一符号を付した構成要素は、第 1 実施形態で説明した同一符号の構成要素と同じである。

【0375】

通信モジュール 162 は、サービスプロバイダ 310 との間の通信処理を行なう。

具体的には、通信モジュール 162 は、サービスプロバイダ 310 から衛星放送などで受信したセキュアコンテンツ 304 を復号モジュール 905 に出力する。また、通信モジュール 162 は、サービスプロバイダ 310 から電話回線などを介して受信したユーザ嗜好フィルタデータ 900 を CAモジュール 311 に出力すると共に、CAモジュール 311 から入力した SP 用購入履歴データ 309 を電話回線などを介してサービスプロバイダ 310 に送信する。

【0376】

図 75 は、CAモジュール 311 および復号モジュール 905 の機能ブロック図である。

図 75 に示すように、CAモジュール 311 は、相互認証部 906、記憶部 907、暗号化・復号部 908 および SP 用購入履歴データ生成部 909 を有する。

相互認証部 906 は、CAモジュール 311 とサービスプロバイダ 310 との間で電話回線を介してデータを送受信する際に、サービスプロバイダ 310 との間で相互認証を行ってセッション鍵データ K_{SES} を生成し、これを暗号化・復号部 908 に出力する。

【0377】

記憶部 907 は、例えば、サービスプロバイダ 310 とユーザとの間で契約が

成立した後に、サービスプロバイダ 310 から IC カード 912 などを用いてオフラインで供給されたマスタ鍵データ K_M を記憶する。

【0378】

暗号化・復号部 908 は、復号モジュール 905 の復号部 910 からそれぞれ暗号化されたスクランブル鍵データ K_{SCR} およびワーク鍵データ K_W を入力し、記憶部 907 から読み出したマスタ鍵データ K_M を用いてワーク鍵データ K_W を復号する。そして、暗号化・復号部 908 は、当該復号したワーク鍵データ K_W を用いてスクランブル鍵データ K_{SCR} を復号し、当該復号したスクランブル鍵データ K_{SCR} を復号部 910 に出力する。

また、暗号化・復号部 908 は、電話回線などを介して通信モジュール 162 がサービスプロバイダ 310 から受信したユーザ嗜好フィルタデータ 900 を、相互認証部 906 からのセッション鍵データ K_{SES} を用いて復号して復号モジュール 905 のセキュアコンテナ選択部 911 に出力する。

また、暗号化・復号部 908 は、SP 用購入履歴データ生成部 909 から入力した SP 用購入履歴データ 309 を、相互認証部 906 からのセッション鍵データ K_{SES} を用いて復号して通信モジュール 162 を介してサービスプロバイダ 310 に送信する。

【0379】

SP 用購入履歴データ生成部 909 は、図 74 に示す購入・利用形態決定操作部 165 を用いてユーザによるコンテンツデータ C の購入操作に応じた操作信号 S165、または SAM305₁ からの利用制御状態データ 166 に基づいて、サービスプロバイダ 310 に固有のコンテンツデータ C の購入履歴を示す SP 用購入履歴データ 309 を生成し、これを暗号化・復号部 908 に出力する。

SP 用購入履歴データ 309 は、例えば、サービスプロバイダ 310 が配信サービスに関してユーザから徴収したい情報、月々の基本料金（ネットワーク家賃）、契約（更新）情報および購入履歴情報などを含む。

【0380】

なお、CA モジュール 311 は、サービスプロバイダ 310 が課金機能を有している場合には、サービスプロバイダ 310 の課金データベース、顧客管理デー

データベースおよびマーケティング情報データベースと通信を行う。この場合に、CAモジュール311は、コンテンツデータの配信サービスについての課金データをサービスプロバイダ310に送信する。

【0381】

復号モジュール905は、復号部910およびセキュアコンテナ選択部911を有する。

復号部910は、通信モジュール162から、それぞれ暗号化されたセキュアコンテナ304、スクランブル鍵データ K_{SCR} およびワーク鍵データ K_W を入力する。

そして、復号部910は、暗号化されたスクランブル鍵データ K_{SCR} およびワーク鍵データ K_W をCAモジュール311の暗号化・復号部908に出力し、暗号化・復号部908から復号されたスクランブル鍵データ K_{SCR} を入力する。

そして、復号部910は、暗号化されたセキュアコンテナ304を、スクランブル鍵データ K_{SCR} を用いて復号した後に、セキュアコンテナ選択部911に出力する。

【0382】

なお、セキュアコンテナ304が、MPEG2 Transport Stream方式でサービスプロバイダ310から送信される場合には、例えば、復号部910は、TS Packet内のECM (Entitlement Control Message) からスクランブル鍵データ K_{SCR} を取り出し、EMM (Entitlement Management Message) からワーク鍵データ K_W を取り出す。

ECMには、その他に、例えば、チャンネル毎の番組属性情報などが含まれている。また、EMMは、その他に、ユーザ（視聴者）毎に異なる個別試聴契約情報などが含まれている。

【0383】

セキュアコンテナ選択部911は、復号部910から入力したセキュアコンテナ304を、CAモジュール311から入力したユーザ嗜好フィルタデータ90

0を用いてフィルタリング処理して、ユーザの嗜好に応じたセキュアコンテナ304を選択してSAM305₁に出力する。

【0384】

次に、SAM305₁について説明する。

なお、SAM305₁は、サービスプロバイダ310についての署名検証処理を行なうなど、コンテンツプロバイダ301に加えてサービスプロバイダ310に関しての処理を行う点を除いて、図26～図41などを用いて前述した第1実施形態のSAM105₁と基本的に行なう機能および構造を有している。

また、SAM305₂～305₄は、SAM305₁と基本的に同じ機能を有している。

すなわち、SAM305₁～305₄は、コンテンツ単位の課金処理をおこなうモジュールであり、EMDサービスセンタ302との間で通信を行う。

【0385】

以下、SAM305₁の機能について詳細に説明する。

図76は、SAM305₁の機能の構成図である。

なお、図76には、サービスプロバイダ310からセキュアコンテナ304を入力する際の処理に関連するデータの流れが示されている。

図76に示すように、SAM305₁は、相互認証部170、暗号化・復号部171、172、173、誤り訂正部181、ダウンロードメモリ管理部182、セキュアコンテナ復号部183、復号・伸長モジュール管理部184、EMDサービスセンタ管理部185、利用監視部186、署名処理部189、SAM管理部190、記憶部192、メディアSAM管理部197、スタックメモリ200、サービスプロバイダ管理部580、課金処理部587、署名処理部598および外部メモリ管理部811を有する。

なお、図76に示すSAM305₁の所定の機能は、SAM105₁の場合と同様に、CPUにおいて秘密プログラムを実行することによって実現される。

図76において、図26と同じ符号を付した機能ブロックは、第1実施形態で説明した同一符号の機能ブロックと同じである。

【0386】

また、図 74 に示す外部メモリ 201 には、第 1 実施形態で説明した処理および後述する処理を経て、利用履歴データ 308 および SAM 登録リストが記憶される。

また、スタックメモリ 200 には、図 77 に示すように、コンテンツ鍵データ K_c 、権利書データ (UCP) 106、記憶部 192 のロック鍵データ K_{LOC} 、コンテンツプロバイダ 301 の公開鍵証明書データ CER_{CP} 、サービスプロバイダ 310 の公開鍵証明書データ CER_{SP} 、利用制御状態データ (UCS) 366、SAM プログラム・ダウンロード・コンテナ $SDC_1 \sim SDC_3$ およびプライスタグデータ 312 などが記憶される。

【0387】

以下、SAM 305₁ の機能ブロックのうち、図 76 において新たに符号を付した機能ブロックについて説明する。

署名処理部 589 は、記憶部 192 あるいはスタックメモリ 200 から読み出した EMD サービスセンタ 302 の公開鍵データ $K_{ESC, P}$ 、コンテンツプロバイダ 301 の公開鍵データ $K_{cp, p}$ び サービスプロバイダ 310 の公開鍵データ $K_{SP, P}$ を用いて、セキュアコンテナ 304 内の署名データの検証を行なう。

【0388】

課金処理部 587 は、図 78 に示すように、図 74 に示す購入・利用形態決定操作部 165 からの操作信号 S_{165} と、スタックメモリ 200 から読み出されたプライスタグデータ 312 とに基づいて、ユーザによるコンテンツの購入・利用形態に応じた課金処理を行う。

課金処理部 587 による課金処理は、利用監視部 186 の監視の下、権利書データ 106 が示す使用許諾条件などの権利内容および利用制御状態データ 166 に基づいて行われる。すなわち、ユーザは、当該権利内容などに従った範囲内でコンテンツの購入および利用を行うことができる。

【0389】

また、課金処理部 587 は、課金処理において、利用履歴データ 308 を生成し、これを外部メモリ管理部 811 を介して外部メモリ 201 に書き込む。

ここで、利用履歴データ 308 は、第 1 実施形態の利用履歴データ 108 と同様に、EMD サービスセンタ 302 において、セキュアコンテナ 304 に関連したライセンス料の支払いを決定する際に用いられる。

【0390】

また、課金処理部 587 は、操作信号 S165 に基づいて、ユーザによるコンテンツの購入・利用形態を記述した利用制御状態 (UCS: Usage Control Status) データ 166 を生成し、これをスタックメモリ 200 に書き込む。

コンテンツの購入形態としては、例えば、購入者による再生や当該購入者の利用のための複製に制限を加えない買い切りや、再生する度に課金を行なう再生課金などがある。

ここで、利用制御状態データ 166 は、ユーザがコンテンツの購入形態を決定したときに生成され、以後、当該決定された購入形態で許諾された範囲内でユーザが当該コンテンツの利用を行なうように制御するために用いられる。利用制御状態データ 166 には、コンテンツの ID、購入形態、買い切り価格、当該コンテンツの購入が行なわれた SAM の SAM_ID、購入を行なったユーザの USER_ID などが記述されている。

【0391】

なお、決定された購入形態が再生課金である場合には、例えば、SAM305₁ からサービスプロバイダ 310 に利用制御状態データ 166 をリアルタイムに送信し、サービスプロバイダ 310 が EMD サービスセンタ 302 に、利用履歴データ 308 を SAM105₁ に取りに行くことを指示する。

また、決定された購入形態が買い切りである場合には、例えば、利用制御状態データ 166 が、サービスプロバイダ 310 および EMD サービスセンタ 302 にリアルタイムに送信される。

【0392】

また、SAM305₁ では、図 76 に示すように、EMD サービスセンタ管理部 185 を介して EMD サービスセンタ 302 から受信したユーザ嗜好フィルタデータ 903 が、サービスプロバイダ管理部 580 に出力される。そして、サー

ビスプロバイダ管理部 580 において、図 74 に示す復号モジュール 905 から入力したセキュアコンテナ 304 のうち、ユーザ嗜好フィルタデータ 903 に基づいてフィルタリングされてユーザの嗜好に応じたセキュアコンテナ 304 が選択され、当該選択されたセキュアコンテナ 304 が誤り訂正部 181 に出力される。これにより、SAM305₁ において、当該 SAM305₁ のユーザが契約している全てのサービスプロバイダ 310 を対象として、当該ユーザによるコンテンツデータ C の購入状況から得られた当該ユーザの嗜好に基づいたコンテンツデータ C の選択処理が可能になる。

【0393】

以下、SAM305₁ 内での処理の流れを説明する。

EMD サービスセンタ 302 から受信した配信用鍵データ KD₁ ~ KD₃ を記憶部 192 に格納する際の SAM305₁ 内での処理の流れは、前述した SAM105₁ の場合と同様である。

【0394】

次に、セキュアコンテナ 304 をサービスプロバイダ 310 から入力する際の SAM305₁ 内での処理の流れを図 76 を参照しながら説明する。

相互認証部 170 と図 63 に示すサービスプロバイダ 310 の相互認証部 352 との間で相互認証が行なわれる。

暗号化・復号部 171 は、当該相互認証によって得られたセッション鍵データ K_{SES} を用いて、サービスプロバイダ管理部 580 を介してサービスプロバイダ 310 から受信した図 65 に示すセキュアコンテナ 304 を復号する。

【0395】

次に、署名処理部 589 は、図 65 (D) に示す署名データ SIG₆₁, ES_C, SIG₁, ES_C の検証を行った後に、公開鍵証明書データ CER_{SP}, CER_{CP} 内に格納された公開鍵データ K_{SP}, P, K_{CP}, P を用いて、署名データ SIG₆, CP, SIG₆₂, SP, SIG₇, CP, SIG₆₃, SP, SIG₆₄, SP の正当性を検証する。

ここで、署名データ SIG₆, CP, SIG₆₂, SP を検証することでコンテンツファイル CF の作成者および送信者の正当性が確認され、署名データ SI

G₇, CP, SIG₆₃, SPを検証することでキーファイルKFの送信者の正当性が確認され、署名データSIG₆₄, SPを検証することでプライスタグデータ312の作成者および送信者の正当性が確認される。

また、署名処理部589は、記憶部192から読み出した公開鍵データK_{ESC}, Pを用いて、図65(B)に示すキーファイルKFに格納された署名データSIG_{K1}, ESCの正当性を検証することで、キーファイルKFの作成者の正当性、並びにキーファイルKFがEMDサービスセンタ302で登録されているか否かを検証する。

【0396】

サービスプロバイダ管理部580は、署名処理部589において上述した全ての署名データの正当性が確認されると、セキュアコンテナ304を誤り訂正部181に出力する。

【0397】

誤り訂正部181は、セキュアコンテナ304を誤り訂正した後に、ダウンロードメモリ管理部182に出力する。

ダウンロードメモリ管理部182は、相互認証部170と図74に示すメディアSAM167aとの間で相互認証を行なった後に、セキュアコンテナ304をダウンロードメモリ167に書き込む。

【0398】

次に、ダウンロードメモリ管理部182は、相互認証部170と図74に示すメディアSAM167aとの間で相互認証を行なった後に、セキュアコンテナ304に格納された図65(B)に示すキーファイルKFをダウンロードメモリ167から読み出してセキュアコンテナ復号部183に出力する。

【0399】

そして、セキュアコンテナ復号部183は、記憶部192から入力した対応する期間の配信用鍵データKD₁~KD₃を用いて、図65(B)に示すキーファイルKFに格納されたコンテンツ鍵データK_c、権利書データ106およびSAMプログラム・ダウンロード・コンテナSDC₁~SDC₃が復号される。

そして、復号されたコンテンツ鍵データK_c、権利書データ106およびSA

Mプログラム・ダウンロード・コンテナSDC₁～SDC₃がスタックメモリ200に書き込まれる。

【0400】

以下、サービスプロバイダ310からダウンロードメモリ167にダウンロードされたセキュアコンテナ304の購入形態を決定するまでの処理の流れを図78および図79を参照しながら説明する。

図79は、セキュアコンテナ304の購入形態決定処理を説明するためのフローチャートである。

<ステップE1>

ユーザによる図74に示す購入・利用形態決定操作部165の操作によって、試聴モードを示す操作信号S165が課金処理部587に出力された場合には、ステップE2の処理が行われ、そうでない場合にはステップE3の処理が行われる。

【0401】

<ステップE2>

試聴モードを示す操作信号S165が課金処理部587に出力された場合に行われ、例えば、ダウンロードメモリ167に記憶されているコンテンツファイルCFが、復号・伸長モジュール管理部184を介して、図74に示す復号・伸長モジュール163に出力される。

このとき、コンテンツファイルCFに対して、相互認証部170とメディアSAM167aとの間の相互認証およびセッション鍵データK_{SES}による暗号化・復号と、相互認証部170と相互認証部220との間の相互認証およびセッション鍵データK_{SES}による暗号化・復号とが行なわれる。

コンテンツファイルCFは、図74に示す復号部221においてセッション鍵データK_{SES}を用いて復号された後に、復号部222に出力される。

【0402】

また、スタックメモリ200から読み出されたコンテンツ鍵データKcおよび半開示パラメータデータ199が、図74に示す復号・伸長モジュール163に出力される。このとき、相互認証部170と相互認証部220との間の相互認証

後に、コンテンツ鍵データ K_c および半開示パラメータデータ 199 に対してセッション鍵データ K_{SES} による暗号化および復号が行なわれる。

次に、復号された半開示パラメータデータ 199 が半開示処理部 225 に出力され、半開示処理部 225 からの制御によって、復号部 222 によるコンテンツ鍵データ K_c を用いたコンテンツデータ C の復号が半開示で行われる。

次に、半開示で復号されたコンテンツデータ C が、伸長部 223 において伸長された後に、電子透かし情報処理部 224 に出力される。

次に、電子透かし情報処理部 224 においてユーザ電子透かし情報用データ 196 がコンテンツデータ C に埋め込まれた後、コンテンツデータ C が再生モジュール 169 において再生され、コンテンツデータ C に応じた音響が出力される。

【0403】

<ステップ E3>

ユーザが、購入・利用形態決定操作部 165 を操作して購入形態を決定すると、当該決定した購入形態を示す操作信号 S_{165} が課金処理部 187 に出力される。

【0404】

<ステップ E4>

課金処理部 187 において、決定された購入形態に応じた利用履歴データ 308 および利用制御状態データ 166 が生成され、利用履歴データ 308 が外部メモリ管理部 811 を介して外部メモリ 201 に書き込まれると共に利用制御状態データ 166 がスタックメモリ 200 に書き込まれる。

以後は、利用監視部 186 において、利用制御状態データ 166 によって許諾された範囲で、コンテンツの購入および利用が行なわれるように制御（監視）される。

そして、スタックメモリ 200 に格納されているキーファイル K_F と、利用制御状態データ 166 とを用いて、購入形態が決定した後述する図 81 (C) に示す新たなキーファイル K_{F1} が生成され、当該作成されたキーファイル K_{F1} がスタックメモリ 200 に記憶される。

図 81 (C) に示すように、キーファイル K_{F1} に格納された利用制御状態デ

ータ166はストレージ鍵データ K_{STR} およびメディア鍵データ K_{MED} を用いてDESのCBCモードを利用して順に暗号化されている。

ここで、記録用鍵データ K_{STR} は、例えばSACD (Super Audio Compact Disc)、DVD (Digital Versatile Disc) 機器、CD-R機器およびMD (Mini Disc) 機器などの種類に応じて決まるデータであり、機器の種類と記録媒体の種類とを1対1で対応づけるために用いられる。また、メディア鍵データ K_{MED} は、記録媒体にユニークなデータである。

【0405】

また、署名処理部589において、 $SAM305_1$ の秘密鍵データ K_{SAM1} 、 S を用いて、キーファイル KF_1 のハッシュ値 H_{K1} が作成され、当該作成されたハッシュ値 H_{K1} が、キーファイル KF_1 と対応付けられて、スタックメモリ200に記憶される。

【0406】

<ステップE5>

$SAM305_1$ からEMDサービスセンタ302に、利用制御状態データ166が送信される。当該利用制御状態データ166の送信は、 $SAM305$ において、コンテンツデータの購入形態が決定される度に行われる。

なお、 $SAM305_1$ からEMDサービスセンタ302への利用履歴データ308の送信は、例えば、例えば、1箇月などの所定の時間間隔で行われる。

【0407】

次に、ダウンロードメモリ167に記憶されている購入形態が既に決定されたコンテンツデータCを再生する場合の処理の流れを、図78を参照しながら説明する。

この場合には、利用監視部186の監視下で、操作信号 $S165$ に基づいて、ダウンロードメモリ167に記憶されているコンテンツファイルCFが、図74に示す復号・伸長モジュール163に出力される。

また、スタックメモリ200から読み出されたコンテンツ鍵データ K_c が復号・伸長モジュール163に出力される。

そして、復号・伸長モジュール 163 の復号部 222 において、コンテンツ鍵データ K_c を用いたコンテンツファイル CF の復号と、伸長部 223 による伸長処理とが行なわれ、再生モジュール 169 において、コンテンツデータ C が再生される。

このとき、課金処理部 587 において、操作信号 $S165$ に応じて、外部メモリ 201 に記憶されている利用履歴データ 308 が更新される。

利用履歴データ 308 は、秘密鍵データ K_{SAM1} , S を用いて作成した署名データ SIG_{205} , $SAM1$ と共に、EMD サービスセンタ管理部 185 を介して、所定のタイミングで、EMD サービスセンタ 302 に送信される。

【0408】

次に、図 80 に示すように、例えば、ネットワーク機器 360₁ のダウンロードメモリ 167 にダウンロードされた既に購入形態が決定された図 81 に示すセキュアコンテナ 304_x を、バス 191 を介して、AV 機器 360₂ の $SAM305_2$ に転送する場合の $SAM305_1$ 内での処理の流れを図 82 を参照しながら説明する。

ユーザは、購入・利用形態決定操作部 165 を操作して、ダウンロードメモリ 167 に記憶された所定のコンテンツを AV 機器 360₂ に転送することを指示し、当該操作に応じた操作信号 $S165$ が、課金処理部 587 に出力される。

これにより、課金処理部 587 は、操作信号 $S165$ に基づいて、スタックメモリ 200 に記憶されている利用履歴データ 308 を更新する。

【0409】

また、ダウンロードメモリ管理部 182 は、ダウンロードメモリ 167 から読み出した図 81 (A), (B), (C) に示すコンテンツファイル CF およびキーファイル KF , KF_1 を署名処理部 589 および SAM 管理部 190 に出力する。

そして、署名処理部 589 は、コンテンツファイル CF およびキーファイル KF の署名データ SIG_{41} , $SAM1$, SIG_{42} , $SAM1$ を作成すると共に、キーファイル KF_1 のハッシュ値 H_{K1} を作成し、これらを SAM 管理部 190 に出力する。

また、SAM管理部190は、図81(D)，(E)に示すプライスタグデータ312およびその署名データSIG₆₄，S_Pと、公開鍵証明書データCER_{C_P}およびその署名データSIG₁，ESCスタックメモリ200から読み出す。

また、SAM管理部190は、図81(E)に示す公開鍵証明書データCER_{SAM1}およびその署名データSIG₂₂，ESCを記憶部192から読み出す。

【0410】

次に、SAM管理部190は、図81に示すセキュアコンテナ304xを作成する。

また、相互認証部170は、SAM305₂との間で相互認証を行って得たセッション鍵データK_{SES}を暗号化・復号部171に出力する。

SAM管理部190は、図81に示すセキュアコンテナ304xを、暗号化・復号部171において、セッション鍵データK_{SES}を用いて暗号化した後に、図82に示すAV機器360₂のSAM305₂に出力する。

【0411】

以下、図80に示すように、SAM305₁から入力したセキュアコンテナ304xを、RAM型などの記録媒体（メディア）に書き込む際のSAM305₂内での処理の流れを、図83を参照しながら説明する。

【0412】

この場合には、SAM305₂のSAM管理部190は、図83に示すように、図81に示すセキュアコンテナ304xを、ネットワーク機器360₁のSAM305₁から入力する。

そして、SAM305₁の相互認証部170とSAM305₂の相互認証部170との間の相互認証が行われ、署名処理部589において、当該相互認証によって得られたセッション鍵データK_{SES}を用いて、セキュアコンテナ304xの復号が行われる。

次に、署名処理部589において、記憶部192から読み出した公開鍵データK_{ESC, P}を用いて、図81(E)に示す署名データSIG₆₁，ESC，S

IG_1, ESC, SIG_{22}, ESC の正当性を検証する。

そして、署名データ $SIG_{61}, ESC, SIG_1, ESC, SIG_{22}, ESC$ の正当性が確認されると、署名処理部589において、公開鍵証明書データ $CER_{SP}, CER_{CP}, CER_{SAM1}$ に含まれる公開鍵データ $K_{SP}, P, K_{CP}, P, K_{SAM1}, P$ を用いて、図81(A)～(D)に示す署名データ

$SIG_6, CP, SIG_{62}, SP, SIG_{41}, SAM1, SIG_7, CP, SIG_{63}, SP, SIG_{42}, SAM1, SIG_{64}, SP$ およびハッシュ値 H_{K1} の正当性が検証される。

そして、これらの署名データの正当性が確認されると、スタックメモリ200に、キーファイル KF, KF_1 およびプライスタグデータ312が記憶される。

また、コンテンツファイル CF が、SAM管理部190から記録モジュール管理部855に出力される。

そして、図81(C)に示すキーファイル KF_1 に格納されたコンテンツ鍵データ K_c および利用制御状態データ166が、スタックメモリ200から暗号化・復号部173に読み出され、暗号化・復号部173において、記憶部192から読み出した記録用鍵データ K_{STR} 、メディア鍵データ K_{MED} および購入者鍵データ K_{PIN} を用いて順に暗号化された後に記録モジュール管理部855に出力される。

また、スタックメモリ200から読み出されたキーファイル KF が、記録モジュール管理部855に出力される。

そして、相互認証部170とRAM型の記録媒体130₄のメディアSAM133との間の相互認証を行った後に、コンテンツファイル CF がRAM型の記録媒体130₄のセキュアでないRAM領域134に記憶され、キーファイル KF, KF_1 およびプライスタグデータ312がセキュアRAM領域132に書き込まれる。

なお、キーファイル KF, KF_1 およびプライスタグデータ312を、RAM型の記録媒体130₄のメディアSAM133に記憶するようにしてもよい。

【0413】

なお、SAM305₁内での処理のうち、コンテンツの購入形態が未決定のR

OM型の記録媒体の購入形態を決定する際のAV機器360₂内での処理の流れ、AV機器360₃において購入形態が未決定のROM型の記録媒体からセキュアコンテナ304を読み出してこれをAV機器360₂に転送してRAM型の記録媒体に書き込む際の処理の流れは、サービスプロバイダ310の秘密鍵データを用いた署名データの署名データの検証を行なう点と、購入形態を決定したキーファイル内にプライスタグデータ312を格納する点を除いて、第1実施形態のSAM105₁の場合と同じである。

【0414】

次に、図59に示すEMDシステム300の全体動作について説明する。

図84および図85は、EMDシステム300の全体動作のフローチャートである。

ここでは、サービスプロバイダ310からユーザホームネットワーク303にオンラインでセキュアコンテナ304を送信する場合を例示して説明する。

なお、以下に示す処理の前提として、EMDサービスセンタ302へのコンテンツプロバイダ301、サービスプロバイダ310およびSAM305₁～305₄の登録は既に終了しているものとする。

【0415】

ステップS21：EMDサービスセンタ302は、コンテンツプロバイダ301の公開鍵データ K_{CP} 、Pの公開鍵証明書 CER_{CP} を、自らの署名データ SIG_1 、 ESC と共にコンテンツプロバイダ301に送信する。

また、EMDサービスセンタ302は、コンテンツプロバイダ301の公開鍵データ K_{SP} 、Pの公開鍵証明書 CER_{SP} を、自らの署名データ SIG_{61} 、 ESC と共にサービスプロバイダ310に送信する。

また、EMDサービスセンタ302は、各々有効期限が1カ月の3カ月分の配信鍵データ $KD_1 \sim KD_3$ をユーザホームネットワーク303のSAM305₁～305₄に送信する。

【0416】

ステップS22：コンテンツプロバイダ301は、相互認証を行った後に、図18に示す登録用モジュール Mod_2 を、EMDサービスセンタ302に送信す

る。

そして、EMDサービスセンタ302は、所定の署名検証を行った後に、権利書データ106およびコンテンツ鍵データKcを登録して権威化する。

また、EMDサービスセンタ302は、登録用モジュールMod₂に応じた図5(B)に示す6カ月分のキーファイルKFを作成し、これをコンテンツプロバイダ301に送信する。

【0417】

ステップS23：コンテンツプロバイダ301は、図5(A)，(B)に示すコンテンツファイルCFおよびその署名データSIG₆，CPと、キーファイルKFおよびその署名データSIG₇，CPとを作成し、これらと図5(C)に示す公開鍵証明書データCER_{cp}およびその署名データSIG₁，ESCとを格納したセキュアコンテナ104を、オンラインおよび／またはオフラインで、サービスプロバイダ310に提供する。

【0418】

ステップS24：サービスプロバイダ310は、図5(C)に示す署名データSIG₁，ESCを検証した後に、公開鍵証明書データCER_{CP}に格納された公開鍵データK_{CP}，Pを用いて、図5(A)，(B)に示す署名データSIG₆，CPおよびSIG₇，CPを検証して、セキュアコンテナ104が正当なコンテンツプロバイダ301から送信されたものであるかを確認する。

【0419】

ステップS25：サービスプロバイダ310は、プライスタグデータ312およびその署名データSIG₆₄，SPを作成し、これらを格納した図65に示すセキュアコンテナ304を作成する。

【0420】

ステップS26：サービスプロバイダ310は、図69に示すプライスタグ登録要求モジュールMod₁₀₂を、EMDサービスセンタ302に送信する。

そして、EMDサービスセンタ302は、所定の署名検証を行った後に、プライスタグデータ312を登録して権威化する。

【0421】

ステップ S 2 7 : サービスプロバイダ 3 1 0 は、例えば、ユーザホームネットワーク 3 0 3 の C A モジュール 3 1 1 からの要求に応じて、ステップ S 2 5 で作成したセキュアコンテナ 3 0 4 を、オンラインあるいはオフラインで、図 7 4 に示すネットワーク機器 3 6 0₁ の復号モジュール 9 0 5 に送信する。

【 0 4 2 2 】

ステップ S 2 8 : C A モジュール 3 1 1 は、S P 用購入履歴データ 3 0 9 を作成し、これを所定のタイミングで、サービスプロバイダ 3 1 0 に送信する。

【 0 4 2 3 】

ステップ S 2 9 : S A M 3 0 5₁ ~ 3 0 5₄ のいずれかにおいて、図 6 5 (D) に示す署名データ S I G₆₁, E S C を検証した後に、公開鍵証明書データ C E R_{S P} に格納された公開鍵データ K_{S P}, P を用いて、図 6 5 (A) , (B) , (C) に示す署名データ S I G₆₂, S P, S I G₆₃, S P, S I G₆₄, S P を検証して、セキュアコンテナ 3 0 4 内の所定のデータが正当なサービスプロバイダ 3 1 0 において作成および送信されたか否かを確認する。

【 0 4 2 4 】

ステップ S 3 0 : S A M 3 0 5₁ ~ 3 0 5₄ のいずれかにおいて、図 6 5 (D) に示す署名データ S I G₁, E S C を検証した後に、公開鍵証明書データ C E R_{C P} に格納された公開鍵データ K_{C P}, P を用いて、図 6 5 (A) , (B) , (C) に示す署名データ S I G₆, S P, S I G₇, S P を検証して、セキュアコンテナ 3 0 4 内のコンテンツファイル C F が正当なコンテンツプロバイダ 3 0 1 において作成されたか否かと、キーファイル K F が正当なコンテンツプロバイダ 3 0 1 から送信されたか否かを確認する。

また、S A M 3 0 5₁ ~ 3 0 5₄ のいずれかにおいて、公開鍵データ K_{E S C}, P を用いて、図 6 5 (B) に示すキーファイル K F 内の署名データ S I G_{K1}, E S C の正当性を検証することで、キーファイル K F が正当な E M D サービスセンタ 3 0 2 によって作成されたか否かを確認する。

【 0 4 2 5 】

ステップ S 3 1 : ユーザが図 7 4 の購入・利用形態決定操作部 1 6 5 を操作してコンテンツの購入・利用形態を決定する。

【0426】

ステップS32：ステップS31において生成された操作信号S165に基づいて、SAM305₁～305₄において、セキュアコンテナ304の利用履歴(Usage Log)データ308が生成される。

SAM305₁～305₄からEMDサービスセンタ302に、利用履歴データ308およびその署名データSIG₂₀₅、SAM₁が送信される。

また、購入形態が決定される度にリアルタイムに、SAM305₁～305₄からEMDサービスセンタ302に利用制御状態データ166が送信される。

【0427】

ステップS33：EMDサービスセンタ302は、利用履歴データ308に基づいて、コンテンツプロバイダ301およびサービスプロバイダ310の各々について、課金内容を決定(計算)し、その結果に基づいて、決済請求権データ152c, 152sを作成する。

【0428】

ステップS34：EMDサービスセンタ302は、ペイメントゲートウェイ90を介して決済機関91に、決済請求権データ152c, 152sを自らの署名データと共に送信し、これにより、ユーザホームネットワーク303のユーザが決済機関91に支払った金銭が、コンテンツプロバイダ301およびサービスプロバイダ310の所有者に分配される。

【0429】

以上説明したように、EMDシステム300では、図5に示すフォーマットのセキュアコンテナ104をコンテンツプロバイダ301からサービスプロバイダ310に配給し、セキュアコンテナ104内のコンテンツファイルCFおよびキーファイルKFをそのまま格納したセキュアコンテナ304をサービスプロバイダ310からユーザホームネットワーク303に配給し、キーファイルKFについての処理をSAM305₁～305₄内で行う。

また、キーファイルKFに格納されたコンテンツ鍵データKcおよび権利書データ106は、配信鍵データKD₁～KD₃を用いて暗号化されており、配信鍵データKD₁～KD₃を保持しているSAM305₁～305₄内でのみ復号さ

れる。そして、SAM305₁～305₄では、耐タンパ性を有するモジュールであり、権利書データ106に記述されたコンテンツデータCの取り扱い内容に基づいて、コンテンツデータCの購入形態および利用形態が決定される。

【0430】

従って、EMDシステム300によれば、ユーザホームネットワーク303におけるコンテンツデータCの購入および利用を、サービスプロバイダ310における処理とは無関係に、コンテンツプロバイダ101の関係者が作成した権利書データ106の内容に基づいて確実に行わせることができる。すなわち、EMDシステム300にれば、権利書データ106をサービスプロバイダ310が管理できないようできる。

そのため、EMDシステム300によれば、異系列の複数のサービスプロバイダ310を介してユーザホームネットワーク303にコンテンツデータCが配給された場合でも、ユーザホームネットワーク303における当該コンテンツデータCについての権利処理を、コンテンツプロバイダ301が作成した共通の権利書データ106に基づいて行わせることができる。

【0431】

また、EMDシステム300では、セキュアコンテナ104、304内の各ファイルおよびデータについて、それらの作成者および送信者の正当性を示す署名データを格納していることから、サービスプロバイダ310およびSAM305₁～305₄において、それらの作成者および送信者の正当性、並びにそれらが改竄されていないか否かなどを確認できる。その結果、コンテンツデータCの不正利用を効果的に回避できる。

【0432】

また、EMDシステム300では、サービスプロバイダ310からユーザホームネットワーク103へのコンテンツデータCの配給を、オンラインおよびオフラインの何れの場合でもセキュアコンテナ304を用いて行うことで、双方の場合において、SAM305₁～305₄におけるコンテンツデータCの権利処理を共通化できる。

【0433】

また、EMDシステム300では、ユーザホームネットワーク303内のネットワーク機器360₁およびAV機器360₂～360₄においてコンテンツデータCを購入、利用、記録および転送する際に、常に権利書データ106に基づいて処理を行うことで、共通の権利処理ルールを採用できる。

例えば、図86に示すように、コンテンツプロバイダ301が提供したコンテンツデータCを、サービスプロバイダ310からユーザホームネットワーク303に、パッケージ流通、デジタル放送、インターネット、専用線、デジタルラジオおよびモバイル通信などの何れの手法（経路）で配信（配給）した場合でも、ユーザホームネットワーク303、303aのSAMにおいて、コンテンツプロバイダ301が作成した権利書データ106に基づいて、共通の権利処理ルールが採用される。

【0434】

また、EMDシステム300によれば、EMDサービスセンタ302が、認証機能、鍵データ管理機能および権利処理（利益分配）機能を有することから、コンテンツの利用に伴ってユーザが支払った金額が、コンテンツプロバイダ301およびEMDサービスセンタ302の所有者に、予め決められた比率に従って確実に分配される。

また、EMDシステム300によれば、同じコンテンツプロバイダ301が供給した同じコンテンツファイルCFについての権利書データ106は、サービスプロバイダ310のサービス形態とは無関係に、そのままSAM305₁～305₄に供給される。従って、SAM305₁～305₄において、権利書データ106に基づいて、コンテンツプロバイダ301の意向通りに、コンテンツファイルCFの利用を行わせることができる。

すなわち、EMDシステム300によれば、コンテンツを用いたサービスおよびユーザによるコンテンツの利用が行われる際に、従来のように監査組織725に頼ることなく、技術的な手段によって、コンテンツプロバイダ301の所有者の権利および利益を確実に守ることができる。

【0435】

以下、上述した第2実施形態のEMDシステム300で採用するセキュアコン

テナなどの配送プロトコルの具体例について説明する。

図87に示すように、コンテンツプロバイダ301において作成されたセキュアコンテナ104は、インターネット(TCP/IP)あるいは専用線(ATM Cell)などのコンテンツプロバイダ用配送プロトコルを用いてサービスプロバイダ310に提供される。

また、サービスプロバイダ310は、セキュアコンテナ104を用いて作成したセキュアコンテナ304を、デジタル放送(MPEG-TS上のXML/SMIL)、インターネット(TCP/IP上のXML/SMIL)あるいはパッケージ流通(記録媒体)などのサービスプロバイダ用配送プロトコルを用いてユーザホームネットワーク303に配給する。

また、ユーザホームネットワーク303、303a内、あるいはユーザホームネットワーク303と303aとの間において、SAM相互間で、セキュアコンテナが、家庭内EC/配信サービス(1394シリアルバス・インターフェイス上のXML/SMIL)や記録媒体などを用いて転送される。

【0436】

以下、図87において、符号A～Gを用いた経路におけるデータ転送に採用される配送プロトコルの一例を詳細に説明する。

図88は、図87に示すコンテンツプロバイダ301とサービスプロバイダ310との間(符号A)でセキュアコンテナ104などを配送するときに採用される配送プロトコルを説明するための図である。

図88に示すように、コンテンツプロバイダ301からサービスプロバイダ310にセキュアコンテナ104などが、IP/IP-SEC層、SSL(Secure Sockets Layer)層、XML(eXtensible Markup Language)/SMIL(Synchronized Multimedia Integration Language)層およびアプリケーション層において共通鍵を用いたセッションを行って配送される。

【0437】

図89は、図87に示すEMDサービスセンタ302とコンテンツプロバイダ301との間(符号B)でキーファイルなどを配送するときに採用される配送プ

ロトコルを説明するための図である。

図 89 に示すように、EMD サービスセンタ 302 からコンテンツプロバイダ 301 にキーファイルなどが、IP/IP-SEC 層、SSL 層およびアプリケーション層において共通鍵を用いたセッションを行って配送される。

【0438】

図 90 は、図に示す EMD サービスセンタ 302 とサービスプロバイダ 310 との間（符号 C）でプライスタグデータ 312 などを配送するときに採用される配送プロトコルを説明するための図である。

図 90 に示すように、EMD サービスセンタ 302 からサービスプロバイダ 310 にプライスタグデータ 312 などが、IP/IP-SEC 層、SSL 層およびアプリケーション層において共通鍵を用いたセッションを行って配送される。

【0439】

図 91 は、図 87 に示すサービスプロバイダ 310 とユーザホームネットワーク 303 との間（符号 D）、ユーザホームネットワーク 303 内（符号 E）で、セキュアコンテナ 304 などを配送するときに採用される配送プロトコルを説明するための図である。

図 91 に示すように、サービスプロバイダ 310 からユーザホームネットワーク 303 のネットワーク機器 360₁ にセキュアコンテナ 304 などが配送される。

このとき、サービスプロバイダ 310 とネットワーク機器 360₁ との間では、MPEG-TS 層、PES 層または DSM-CC_Data_Carousel 層、および、MHEG (Multimedia and Hypermedia Experts) 層または「http 層および XML/SMIL 層」が、セキュアコンテナ 304 を転送するためのサービスプロバイダ用商品配送プロトコルとして用いられる。

また、ネットワーク機器 360₁ とストレージ機器 360₂ との間、並びに AV 機器相互間では、HAVi (XML) が、セキュアコンテナを転送するためのユーザホームネットワーク商品配送プロトコルとして用いられる。

このとき、デジタル放送のデータ放送方式に XML/SMIL/BML を利用

した場合には、セキュアコンテナ 304 のコンテンツファイル CF1, CF2 およびキーファイル KF1, KF2 と視聴（デモ）サンプルは、図 9 2 に示すように HTTP 層上の BML/XML/SMIL 層およびモノメディアデータ層に格納されて配送される。

また、デジタル放送のデータ放送方式に MHEG を利用した場合には、セキュアコンテナ 304 のコンテンツファイル CF1, CF2 およびキーファイル KF1, KF2 と視聴（デモ）サンプルは、図 9 3 に示すように MHEG 層上のモノメディアデータ層に格納されて配送される。

また、デジタル放送のデータ放送方式に XML/SMIL を利用した場合には、セキュアコンテナ 304 のコンテンツファイル CF1, CF2 およびキーファイル KF1, KF2 と視聴（デモ）サンプルは、図 9 4 に示すように HTTP 層上の XML/SMIL 層に格納されて配送される。

【0440】

図 9 5 は、図 8 7 に示す EMD サービスセンタ 302 とユーザホームネットワーク 303, 303a との間（符号 G）で、利用履歴データ 308 および利用制御状態データ 166 などを配送するときに採用される配送プロトコルを説明するための図である。

図 9 5 に示すように、ネットワーク機器 360₁ から EMD サービスセンタ 302 に、利用履歴データ 308 などが転送される場合に、IP/IP-SEC 層、SSL 層およびアプリケーション層において、セッション鍵データを用いたセッションが行われる。

また、ネットワーク機器 360₂ などが EMD サービスセンタ 302 に利用履歴データ 308 および利用制御状態データ 166 などを転送する場合には、利用履歴データ 308 などが、IP/IP-SEC 層および HAVi 層でセッションを行ってストレージ機器 360₂ からネットワーク機器 360₁ に転送された後に、ネットワーク機器 360₁ から EMD サービスセンタ 302 に前述したように転送される。

【0441】

図 9 6 は、図 8 7 に示すユーザホームネットワーク 303 のストレージ機器 3

60₄ からユーザホームネットワーク 303a のストレージ機器 360₁₁ に、セキュアコンテナを配送するときに採用される配送プロトコルを説明するための図である。

図 9 6 に示すように、ストレージ機器 360₄ からストレージ機器 360₁₁ にセキュアコンテナが、IP/IP-SEC 層、SSL 層、XML/SMIL 層およびアプリケーション層において共通鍵を用いたセッションを行って配送される。

【0442】

第 2 実施形態の第 1 変形例

図 9 7 は、第 2 実施形態の第 1 変形例に係わる 2 個のサービスプロバイダを用いた EMD システム 300a の構成図である。

図 9 7 において、図 5 9 と同一符号を付した構成要素は、第 1 実施形態で説明した同一符号の構成要素と同じである。

図 9 7 に示すように、EMD システム 300a では、コンテンツプロバイダ 301 からサービスプロバイダ 310a および 310b に、同じセキュアコンテナ 104 を供給する。

【0443】

サービスプロバイダ 310a は、例えば、コンテンツをドラマ番組の提供サービスを行っており、当該サービスにおいて、当該ドラマ番組に関連するコンテンツデータ C と、当該コンテンツデータ C について独自に作成したプライスタグデータ 312a とを格納したセキュアコンテナ 304a を作成し、これをネットワーク機器 360₁ に配給する。

また、サービスプロバイダ 310b は、例えば、カラオケサービスを提供しており、当該サービスにおいて、当該カラオケサービスに関連するコンテンツデータ C と、当該コンテンツデータ C について独自に作成したプライスタグデータ 312b とを格納したセキュアコンテナ 304b を作成し、これをネットワーク機器 360₁ に配給する。

ここで、セキュアコンテナ 304a、304b のフォーマットは、図 6 5 を用いた説明したセキュアコンテナ 304 と同じである。

【0444】

ネットワーク機器360a₁には、サービスプロバイダ310a, 310bの各々に対応したCAモジュール311a, 311bが設けられている。

CAモジュール311a, 311bは、自らの要求に応じたセキュアコンテナ304a, 304bの配給を、それぞれサービスプロバイダ310a, 310bから受ける。

【0445】

次に、CAモジュール311a, 311bは、配給されたセキュアコンテナ304a, 304bに応じたSP用購入履歴データ309a, 309bをそれぞれ作成し、これらをそれぞれサービスプロバイダ310a, 310bに送信する。

また、CAモジュール311a, 311bは、セキュアコンテナ304a, 304bをセッション鍵データK_{SES}で復号した後に、SAM305₁~305₄に出力する。

【0446】

次に、SAM305₁~305₄において、共通の配信用鍵データKD₁~KD₃を用いて、セキュアコンテナ304a, 304b内のキーファイルKFが復号され、共通の権利書データ106に基づいて、ユーザからの操作に応じたコンテンツの購入・利用に関する処理が行われ、それに応じた利用履歴データ308が作成される。

【0447】

そして、SAM305₁~305₄からEMDサービスセンタ302に、利用履歴データ308が送信される。

【0448】

EMDサービスセンタ302では、利用履歴データ308に基づいて、コンテンツプロバイダ301およびサービスプロバイダ310a, 310bの各々について、課金内容を決定(計算)し、その結果に基づいて、それぞれに対応する決済請求権データ152c, 152sa, 152sbを作成する。

【0449】

EMDサービスセンタ302は、ペイメントゲートウェイ90を介して決済機

関 9 1 に、決済請求権データ 1 5 2 c, 1 5 2 s a, 1 5 2 s b を送信し、これにより、ユーザホームネットワーク 3 0 3 のユーザが決済機関 9 1 に支払った金銭が、コンテンツプロバイダ 3 0 1 およびサービスプロバイダ 3 1 0 a, 3 1 0 b の所有者に分配される。

【 0 4 5 0 】

上述したように、EMD システム 3 0 0 a によれば、同じコンテンツファイル C F をサービスプロバイダに 3 1 0 a, 3 1 0 b に供給する場合に、当該コンテンツファイル C F についての権利書データ 1 0 6 を配信用鍵データ K D₁ ~ K D₆ で暗号化してサービスプロバイダに 3 1 0 a, 3 1 0 b に供給し、サービスプロバイダに 3 1 0 a, 3 1 0 b は暗号化された権利書データ 1 0 6 をそのまま格納したセキュアコンテナ 3 0 4 a, 3 0 4 b をユーザホームネットワークに配給する。そのため、ユーザホームネットワーク内の S A M 3 0 5₁ ~ 3 0 5₄ では、コンテンツファイル C F をサービスプロバイダに 3 1 0 a, 3 1 0 b の何れから配給を受けた場合でも、共通の権利書データ 1 0 6 に基づいて権利処理を行うことができる。

【 0 4 5 1 】

なお、上述した第 1 変形例では、2 個のサービスプロバイダを用いた場合を例示したが、本発明では、サービスプロバイダの数は任意である。

【 0 4 5 2 】

第 2 実施形態の第 2 変形例

図 9 8 は、第 2 実施形態の第 2 変形例に係わる複数のコンテンツプロバイダを用いた EMD システム 3 0 0 b の構成図である。

図 9 8 において、図 5 9 と同一符号を付した構成要素は、第 1 実施形態で説明した同一符号の構成要素と同じである。

図 9 8 に示すように、EMD システム 3 0 0 b では、EMD サービスセンタ 3 0 2 からコンテンツプロバイダ 3 0 1 a, 3 0 1 b にそれぞれキーファイル K F a, K F b が供給され、コンテンツプロバイダ 3 0 1 a, 3 0 1 b からサービスプロバイダ 3 1 0 に、それぞれセキュアコンテナ 1 0 4 a, 1 0 4 b が供給される。

【0453】

サービスプロバイダ310は、例えば、コンテンツプロバイダ301a, 301bが供給したコンテンツを用いてサービスを提供しており、セキュアコンテナ104aについてのプライスタグデータ312aと、セキュアコンテナ104bについてのプライスタグデータ312bとをそれぞれ生成し、これらを格納したセキュアコンテナ304cを作成する。

図98に示すように、セキュアコンテナ304cには、コンテンツファイルCFa, CFb、キーファイルKF a, KF b、プライスタグデータ312a, 312b、それらの各々についてのサービスプロバイダ310の秘密鍵データ $K_{C_P, S}$ による署名データが格納されている。

【0454】

セキュアコンテナ304cは、ユーザホームネットワーク303のネットワーク機器360₁のCAモジュール311で受信された後に、SAM305₁~305₄において処理される。

【0455】

SAM305₁~305₄では、配信用鍵データKD a₁~KD a₃を用いて、キーファイルKF aが復号され、権利書データ106aに基づいて、コンテンツファイルCF aについてのユーザからの操作に応じた購入・利用に関する処理が行われ、その履歴が利用履歴データ308に記述される。

また、SAM305₁~305₄において、配信用鍵データKD b₁~KD b₃を用いて、キーファイルKF bが復号され、権利書データ106bに基づいて、コンテンツファイルCF bについてのユーザからの操作に応じた購入・利用に関する処理が行われ、その履歴が利用履歴データ308に記述される。

【0456】

そして、SAM305₁~305₄からEMDサービスセンタ302に、利用履歴データ308が送信される。

【0457】

EMDサービスセンタ302では、利用履歴データ308に基づいて、コンテンツプロバイダ301a, 301bおよびサービスプロバイダ310の各々につ

いて、課金内容を決定（計算）し、その結果に基づいて、それぞれに対応する決済請求権データ 152ca, 152cb, 152s を作成する。

【0458】

EMDサービスセンタ 302 は、ペイメントゲートウェイ 90 を介して決済機関 91 に、決済請求権データ 152ca, 152cb, 152s を送信し、これにより、ユーザホームネットワーク 303 のユーザが決済機関 91 に支払った金銭が、コンテンツプロバイダ 301a, 301b およびサービスプロバイダ 310 の所有者に分配される。

【0459】

上述したように、EMDシステム 300b によれば、セキュアコンテナ 304c 内に格納されたコンテンツファイル CFa, CFb の権利書データ 106a, 106b は、コンテンツプロバイダ 301a, 301b が作成したものをそのまま用いるため、SAM 305₁ ~ 305₄ 内において、権利書データ 106a, 106b に基づいて、コンテンツファイル CFa, CFb についての権利処理がコンテンツプロバイダ 301a, 301b の意向に沿って確実に行われる。

【0460】

なお、図 98 に示す第 2 変形例では、2 個のコンテンツプロバイダを用いた場合を例示したが、コンテンツプロバイダの数は任意である。

また、コンテンツプロバイダおよびサービスプロバイダの双方が複数であってもよい。

【0461】

第 2 実施形態の第 3 変形例

図 99 は、第 2 実施形態の第 3 変形例に係わる EMD システムの構成図である。

上述した第 2 実施形態では、EMD サービスセンタ 302 が決済機関 91 に対して、コンテンツプロバイダ 301 およびサービスプロバイダ 310 の決済を行う場合を例示したが、本発明では、例えば、図 99 に示すように、EMD サービスセンタ 302 において、利用履歴データ 308 に基づいて、コンテンツプロバイダ 301 のための決済請求権データ 152c と、サービスプロバイダ 310 の

ための決済請求権データ 152 s とを作成し、これらをそれぞれコンテンツプロバイダ 301 およびサービスプロバイダ 310 に送信するようにしてもよい。

この場合には、コンテンツプロバイダ 301 は、決済請求権データ 152 c を用いて、ペイメントゲートウェイ 90 a を介して決済機関 91 a に決済を行う。
また、サービスプロバイダ 310 は、決済請求権データ 152 s を用いて、ペイメントゲートウェイ 90 b を介して決済機関 91 b に決済を行う。

【0462】

第2実施形態の第4変形例

図 100 は、第2実施形態の第4変形例に係わる EMD システムの構成図である。

上述した第2実施形態では、例えば現行のインターネットのようにサービスプロバイダ 310 が課金機能を有していない場合を例示したが、現行のデジタル放送などのようにサービスプロバイダ 310 が課金機能を有している場合には、C A モジュール 311 において、セキュアコンテナ 304 に関するサービスプロバイダ 310 のサービスに対しての利用履歴データ 308 s を作成してサービスプロバイダ 310 に送信する。

そして、サービスプロバイダ 310 は、利用履歴データ 308 s に基づいて、課金処理を行って決済請求権データ 152 s を作成し、これを用いてペイメントゲートウェイ 90 b を介して決済機関 91 b に決済を行う。

一方、SAM 305₁ ~ 305₄ は、セキュアコンテナ 304 に関するコンテンツプロバイダ 301 の権利処理に対しての利用履歴データ 308 c を作成し、これを EMD サービスセンタ 302 に送信する。

EMD サービスセンタ 302 は、利用履歴データ 308 c に基づいて、決済請求権データ 152 c を作成し、これをコンテンツプロバイダ 301 に送信する。

コンテンツプロバイダ 301 は、決済請求権データ 152 c を用いて、ペイメントゲートウェイ 90 a を介して決済機関 91 a に決済を行う。

【0463】

第2実施形態の第5変形例

上述した実施形態では、図 72 に示すように、EMD サービスセンタ 302 の

ユーザ嗜好フィルタ生成部 901 において、SAM305₁ などから受信した利用履歴データ 308 に基づいて、ユーザ嗜好フィルタデータ 903 を生成する場合を例示したが、例えば、図 78 に示す SAM305₁ などの利用監視部 186 で生成されてリアルタイムに EMD サービスセンタ 302 に送信された利用制御状態データ 166 に基づいて、ユーザ嗜好フィルタ生成部 901 においてユーザ嗜好フィルタデータ 903 を生成してもよい。

【0464】

第 2 実施形態の第 6 変形例

コンテンツプロバイダ 301、サービスプロバイダ 310 および SAM305₁ ~ 305₄ は、それぞれ自らの公開鍵データ $K_{CP, P}$, $K_{SP, P}$, $K_{SAM1, P}$ ~ $K_{SAM4, P}$ の他に、自らの秘密鍵データ $K_{CP, S}$, $K_{SP, S}$, $K_{SAM1, S}$ ~ $K_{SAM4, S}$ を EMD サービスセンタ 302 に登録してもよい。

このようにすることで、EMD サービスセンタ 302 は、緊急時に、国家あるいは警察機関などからの要請に応じて、秘密鍵データ $K_{CP, S}$, $K_{SP, S}$, $K_{SAM1, S}$ ~ $K_{SAM4, S}$ を用いて、コンテンツプロバイダ 301 とサービスプロバイダ 310 との間の通信、サービスプロバイダ 310 と SAM305₁ ~ 305₄ との間の通信、並びにユーザホームネットワーク 303 内での SAM305₁ ~ 305₄ 相互間での通信のうち対象となる通信を盗聴することが可能になる。

また、SAM305₁ ~ 305₄ については、出荷時に、EMD サービスセンタ 302 によって秘密鍵データ $K_{SAM1, S}$ ~ $K_{SAM4, S}$ を生成し、これを SAM305₁ ~ 305₄ に格納すると共に EMD サービスセンタ 302 が保持（登録）するようにしてもよい。

【0465】

第 2 実施形態の第 7 変形例

上述した実施形態では、コンテンツプロバイダ 301、サービスプロバイダ 310 および SAM305₁ ~ 305₄ が、相互に通信を行う場合に、EMD サービスセンタ 302 から事前に公開鍵証明書データ CER_{CP} , CER_{SP} , CER_{SAM1} ~ CER_{SAM4} を提供し、これらを用いて公開鍵暗号化を行うようにしてもよい。

$R_{SAM1} \sim CER_{SAN4}$ を取得し、イン・バンド方式で通信先に送信する場合を例示したが、本発明では、通信先への公開鍵証明書データの送信形態として種々の形態を採用できる。

例えば、コンテンツプロバイダ301、サービスプロバイダ310およびSAM305₁～305₄が、相互に通信を行う場合に、EMDサービスセンタ302から事前に公開鍵証明書データ CER_{CP} 、 CER_{SP} 、 $CER_{SAM1} \sim CER_{SAN4}$ を取得し、当該通信に先立ってアウト・オブ・バンド方式で通信先に送信してもよい。

また、コンテンツプロバイダ301、サービスプロバイダ310およびSAM305₁～305₄が、通信時に、EMDサービスセンタ302から公開鍵証明書データ CER_{CP} 、 CER_{SP} 、 $CER_{SAM1} \sim CER_{SAN4}$ を取得してもよい。

【0466】

図101は、公開鍵証明書データの取得（入手）ルートの形態を説明するための図である。

なお、図101において、図59と同じ符号を付した構成要素は、前述した同一符号の構成要素と同じである。また、ユーザホームネットワーク303aは、前述したユーザホームネットワーク303と同じである。ユーザホームネットワーク303bでは、IEEE1394シリアルバスであるバス191を介してSAM305₁₁～305₁₄を接続している。

【0467】

コンテンツプロバイダ301がサービスプロバイダ310の公開鍵証明書データ CER_{SP} を取得する場合には、例えば、通信に先立ってサービスプロバイダ310からコンテンツプロバイダ301に公開鍵証明書データ CER_{SP} を送信する場合（図101中（3））と、コンテンツプロバイダ301がEMDサービスセンタ302から公開鍵証明書データ CER_{SP} を取り寄せる場合（図101中（1））とがある。

【0468】

また、サービスプロバイダ310がコンテンツプロバイダ301の公開鍵証明

書データ CER_{CP} を取得する場合には、例えば、通信に先立ってコンテンツプロバイダ 301 からサービスプロバイダ 310 に公開鍵証明書データ CER_{CP} を送信する場合（図 101 中（2））と、サービスプロバイダ 310 が EMD サービスセンタ 302 から公開鍵証明書データ CER_{CP} を取り寄せる場合（図 101 中（4））とがある。

【0469】

また、サービスプロバイダ 310 が $SAM305_1 \sim 305_4$ の公開鍵証明書データ $CER_{SAM1} \sim CER_{SAM4}$ を取得する場合には、例えば、通信に先立って $SAM305_1 \sim 305_4$ からサービスプロバイダ 310 に公開鍵証明書データ $CER_{SAM1} \sim CER_{SAM4}$ を送信する場合（図 101 中（6））と、サービスプロバイダ 310 が EMD サービスセンタ 302 から公開鍵証明書データ $CER_{SAM1} \sim CER_{SAM4}$ を取り寄せる場合（図 101 中（4））とがある。

【0470】

また、 $SAM305_1 \sim 305_4$ がサービスプロバイダ 310 の公開鍵証明書データ CER_{SP} を取得する場合には、例えば、通信に先立ってサービスプロバイダ 310 から $SAM305_1 \sim 305_4$ に公開鍵証明書データ CER_{SP} を送信する場合（図 101 中（5））と、 $SAM305_1 \sim 305_4$ が EMD サービスセンタ 302 から公開鍵証明書データ CER_{SP} を取り寄せる場合（図 101 中（7）など）とがある。

【0471】

また、 $SAM305_1$ が $SAM305_2$ の公開鍵証明書データ CER_{SAM2} を取得する場合には、例えば、通信に先立って $SAM305_2$ から $SAM305_1$ に公開鍵証明書データ CER_{SAM2} を送信する場合（図 101 中（8））と、 $SAM305_1$ が EMD サービスセンタ 302 から公開鍵証明書データ CER_{SAM2} を取り寄せる場合（図 101 中（7）など）とがある。

【0472】

また、 $SAM305_2$ が $SAM305_1$ の公開鍵証明書データ CER_{SAM1} を取得する場合には、例えば、通信に先立って $SAM305_1$ から $SAM305_2$

2に公開鍵証明書データ CER_{SAM1} を送信する場合(図101中(9))と、 $SAM305_2$ が自らEMDサービスセンタ302から公開鍵証明書データ CER_{SAM1} を取り寄せる場合と、 $SAM305_1$ が搭載されたネットワーク機器を介して公開鍵証明書データ CER_{SAM1} を取り寄せる場合(図101中(7)、(8))とがある。

【0473】

また、 $SAM305_4$ が $SAM305_{13}$ の公開鍵証明書データ $CER_{SAM_{13}}$ を取得する場合には、例えば、通信に先立って $SAM305_{13}$ から $SAM305_4$ に公開鍵証明書データ $CER_{SAM_{13}}$ を送信する場合(図101中(12))と、 $SAM305_4$ が自らEMDサービスセンタ302から公開鍵証明書データ $CER_{SAM_{13}}$ を取り寄せる場合(図101中(10))と、ユーザホームネットワーク303b内のネットワーク機器を介して公開鍵証明書データ $CER_{SAM_{13}}$ を取り寄せる場合とがある。

【0474】

また、 $SAM305_{13}$ が $SAM305_4$ の公開鍵証明書データ CER_{SAM_4} を取得する場合には、例えば、通信に先立って $SAM305_4$ から $SAM305_{13}$ に公開鍵証明書データ CER_{SAM_4} を送信する場合(図101中(11))と、 $SAM305_{13}$ が自らEMDサービスセンタ302から公開鍵証明書データ CER_{SAM_4} を取り寄せる場合(図101中(13))と、ユーザホームネットワーク303b内のネットワーク機器を介して公開鍵証明書データ CER_{SAM_4} を取り寄せる場合とがある。

【0475】

第2実施形態における公開鍵証明書破棄リスト(データ)の取り扱い

第2実施形態では、EMDサービスセンタ302において、不正行為などに用いられたコンテンツプロバイダ301、サービスプロバイダ310および $SAM305_1 \sim 305_4$ が他の装置と通信できないようにするために、当該不正行為に用いられた装置の公開鍵証明書データを無効にする公開鍵証明書破棄データを作成する。そして、当該公開鍵証明書破棄データCRL(Certificate Revocation List)を、コンテンツプロバイダ301、サー

ビスプロバイダ 310 および SAM305₁ ~ 305₄ に送信する。

なお、公開鍵証明書破棄データ CRL は、EMD サービスセンタ 302 の他に、例えば、コンテンツプロバイダ 301、サービスプロバイダ 310 および SAM305₁ ~ 305₄ において生成してもよい。

【0476】

先ず、EMD サービスセンタ 302 が、コンテンツプロバイダ 301 の公開鍵証明書データ CER_{CP} を無効にする場合について説明する。

図 102 に示すように、EMD サービスセンタ 302 は、公開鍵証明書データ CER_{CP} を無効にすることを示す公開鍵証明書破棄データ CRL₁ をサービスプロバイダ 310 に送信する（図 102 中（1））。サービスプロバイダ 310 は、コンテンツプロバイダ 301 から入力した署名データを検証する際に、公開鍵証明書破棄データ CRL₁ を参照して公開鍵証明書データ CER_{CP} の有効性を判断し、有効であると判断した場合に公開鍵データ K_{CP}, P を用いた署名検証を行い、無効であると判断した場合に当該署名検証を行わずにコンテンツプロバイダ 301 からのデータを無効にする。なお、データを無効にするのではなく、通信を拒絶するようにしてもよい。

【0477】

また、EMD サービスセンタ 302 は、公開鍵証明書破棄データ CRL₁ を、サービスプロバイダ 310 の流通資源を利用して放送型あるいはオンデマンド型のいずれか一方で、ユーザホームネットワーク 303 内の例えば SAM305₁ に送信する（図 102 中（1）,（2））。SAM305₁ は、サービスプロバイダ 310 から入力したセキュアコンテナ内に格納されたコンテンツプロバイダ 301 の署名データを検証する際に、公開鍵証明書破棄データ CRL₁ を参照して公開鍵証明書データ CER_{CP} の有効性を判断し、有効であると判断した場合に公開鍵データ K_{CP}, P を用いた署名検証を行い、無効であると判断した場合に当該署名検証を行わずに当該セキュアコンテナを無効にする。

なお、EMD サービスセンタ 302 は、公開鍵証明書破棄データ CRL₁ を、ユーザホームネットワーク 303 内のネットワーク機器を介して SAM305₁ に直接送信してもよい（図 102 中（3））。

【0478】

次に、EMDサービスセンタ302が、サービスプロバイダ310の公開鍵証明書データ CER_{SP} を無効にする場合について説明する。

図103に示すように、EMDサービスセンタ302は、公開鍵証明書データ CER_{SP} を無効にすることを示す公開鍵証明書破棄データ CRL_2 をコンテンツプロバイダ301に送信する（図103中（1））。コンテンツプロバイダ301は、サービスプロバイダ310から入力した署名データを検証する際に、公開鍵証明書破棄データ CRL_2 を参照して公開鍵証明書データ CER_{SP} の有効性を判断し、有効であると判断した場合に公開鍵データ $K_{SP, P}$ を用いた署名検証を行い、無効であると判断した場合に当該署名検証を行わずにサービスプロバイダ310からのデータを無効にする。

【0479】

また、EMDサービスセンタ302は、公開鍵証明書破棄データ CRL_2 を、サービスプロバイダ310の流通資源を利用して放送型あるいはオンデマンド型のいずれか一方で、ユーザホームネットワーク303内の例えば $SAM305_1$ に送信する（図103中（2））。 $SAM305_1$ は、サービスプロバイダ310から入力したセキュアコンテナ内に格納されたサービスプロバイダ310の署名データを検証する際に、公開鍵証明書破棄データ CRL_2 を参照して公開鍵証明書データ CER_{SP} の有効性を判断し、有効であると判断した場合に公開鍵データ $K_{SP, P}$ を用いた署名検証を行い、無効であると判断した場合に当該署名検証を行わずに当該セキュアコンテナを無効にする。

この場合に、サービスプロバイダ310内において、公開鍵証明書破棄データ CRL_2 の送受信を行うモジュールは、耐タンパ性を有している必要がある。また、サービスプロバイダ310内において、公開鍵証明書破棄データ CRL_2 は、サービスプロバイダ310の関係者による改竄な困難な領域に格納される必要がある。

なお、EMDサービスセンタ302は、公開鍵証明書破棄データ CRL_2 を、ユーザホームネットワーク303内のネットワーク機器を介して $SAM305_1$ に直接送信してもよい（図103中（3））。

【0480】

次に、EMDサービスセンタ302が、例えばSAM305₂の公開鍵証明書データCER_{SAM2}を無効にする場合について説明する。

図104に示すように、EMDサービスセンタ302は、公開鍵証明書データCER_{SAM2}を無効にすることを示す公開鍵証明書破棄データCRL₃をコンテンツプロバイダ301に送信する(図104中(1))。コンテンツプロバイダ301は、公開鍵証明書破棄データCRL₃をサービスプロバイダ310に送信する。サービスプロバイダ310は、自らの流通資源を利用して放送型あるいはオンデマンド型のいずれか一方で、ユーザホームネットワーク303内の例えばSAM305₁に公開鍵証明書破棄データCRL_{SAM1}を送信する(図104中(1))。SAM305₁は、SAM305₂から入力したデータに付加されたSAM305₂の署名データを検証する際に、公開鍵証明書破棄データCRL₃を参照して公開鍵証明書データCER_{SAM2}の有効性を判断し、有効であると判断した場合に公開鍵データK_{SAM2, P}を用いた署名検証を行い、無効であると判断した場合に当該署名検証を行わずに当該データを無効にする。

この場合に、サービスプロバイダ310内において、公開鍵証明書破棄データCRL₃の送受信を行うモジュールは、耐タンパ性を有している必要がある。また、サービスプロバイダ310内において、公開鍵証明書破棄データCRL₃は、サービスプロバイダ310の関係者による改竄な困難な領域に格納される必要がある。

【0481】

EMDサービスセンタ302は、公開鍵証明書破棄データCRL₃をサービスプロバイダ310を介してSAM305₁に送信してもよい(図104中(1)、(2))。

また、EMDサービスセンタ302は、公開鍵証明書破棄データCRL₃を、ユーザホームネットワーク303内のネットワーク機器を介してSAM305₁に直接送信してもよい(図104中(3))。

【0482】

また、EMDサービスセンタ302は、例えばSAM305₂の公開鍵証明書

データCER_{SAM2}を無効にすることを示す公開鍵証明書破棄データCRL₃を作成し、これを保管する。

また、ユーザホームネットワーク303は、バス191に接続されているSAMのSAM登録リストSRLを作成し、これをEMDサービスセンタ302に送信する(図105中(1))。

EMDサービスセンタ302は、SAM登録リストに示されるSAM305₁~305₄のうち、公開鍵証明書破棄データCRL₃によって無効にすることが示されているSAM(例えばSAM305₂)を特定し、SAM登録リストSRL内の当該SAMに対応する破棄フラグを無効を示すように設定して新たなSAM登録リストSRLを作成する。

次に、EMDサービスセンタ302は、当該生成したSAM登録リストSRLをSAM305₁に送信する(図105中(1))。

SAM305₁は、他のSAMと通信を行う際に、SAM登録リストSRLの破棄フラグを参照して、署名データの検証の有無および通信を許否するか否かを決定する。

【0483】

また、EMDサービスセンタ302は、公開鍵証明書破棄データCRL₃を作成し、これをコンテンツプロバイダ301に送信する(図105中(2))。

コンテンツプロバイダ301は、公開鍵証明書破棄データCRL₃をサービスプロバイダ310に送信する(図105中(2))。

次に、サービスプロバイダ310は、自らの流通資源を利用して放送型あるいはオンデマンド型のいずれか一方で、公開鍵証明書破棄データCRL₃をSAM305₁に送信する(図105中(2))。

SAM305₁は、自らが作成したSAM登録リストに示されるSAM305₁~305₄のうち、公開鍵証明書破棄データCRL₃によって無効にすることが示されているSAM(例えばSAM305₂)を特定し、SAM登録リストSRL内の当該SAMに対応する破棄フラグを無効を示すように設定する。

以後、SAM305₁は、他のSAMと通信を行う際に、当該SAM登録リストSRLの破棄フラグを参照して、署名データの検証の有無および通信を許否す

るか否かを決定する。

【0484】

また、EMDサービスセンタ302は、公開鍵証明書破棄データCRL₃を作成し、これをサービスプロバイダ310に送信する（図105中（3））。

次に、サービスプロバイダ310は、自らの流通資源を利用して放送型あるいはオンデマンド型のいずれか一方で、公開鍵証明書破棄データCRL₃をSAM305₁に送信する（図105中（3））。

SAM305₁は、自らが作成したSAM登録リストに示されるSAM305₁～305₄のうち、公開鍵証明書破棄データCRL₃によって無効にすることが示されているSAM（例えばSAM305₂）を特定し、SAM登録リストSRL内の当該SAMに対応する破棄フラグを無効を示すように設定する。

以後、SAM305₁は、他のSAMと通信を行う際に、当該SAM登録リストSRLの破棄フラグを参照して、署名データの検証の有無および通信を許否するか否かを決定する。

【0485】

EMDサービスセンタ302の役割等

図106は、図59に示すEMDサービスセンタ（クリアリングハウス）302の機能を権利管理用クリアリングハウス950と、電子決済用クリアリングハウス951とに分割した場合のEMDシステムの構成図である。

当該EMDシステムでは、電子決済用クリアリングハウス951において、ユーザホームネットワーク303a、303bのSAMからの利用履歴データ308に基づいて、決済処理（利益分配処理）を行い、コンテンツプロバイダ301およびサービスプロバイダ310の決済請求権データをそれぞれ生成し、ペイメントゲートウェイ90を介して決済機関91において決済を行う。

【0486】

また、権利管理用クリアリングハウス950は、電子決済用クリアリングハウス951からの決済通知に応じたコンテンツプロバイダ301およびサービスプロバイダ310の決済レポートを作成し、それらをコンテンツプロバイダ301およびコンテンツプロバイダ301に送信する。

また、コンテンツプロバイダ 301 の権利書データ 106 およびコンテンツ鍵データ Kc の登録（権威化）などを行う。

なお、図 107 に示すように、権利管理用クリアリングハウス 950 と電子決済用クリアリングハウス 951 とを単体の装置内に収納すると、図 59 に示す EMD サービスセンタ 302 となる。

【0487】

また、本発明は、例えば、図 108 に示すように、EMD サービスセンタ 302 に、権利管理用クリアリングハウス 960 の機能を設け、権利管理用クリアリングハウス 960 において、権利書データ 106 の登録などを行うと共に、SAM からの利用履歴データ 308 に基づいてサービスプロバイダ 310 の決済請求権データを作成し、これをサービスプロバイダ 310 に送信してもよい。この場合には、サービスプロバイダ 310 は、自らの課金システムを電子決済用クリアリングハウス 961 として利用し、権利管理用クリアリングハウス 960 からの決済請求権データに基づいて決済を行う。

【0488】

また、本発明は、例えば、図 109 に示すように、EMD サービスセンタ 302 に、権利管理用クリアリングハウス 970 の機能を設け、権利管理用クリアリングハウス 970 において、権利書データ 106 の登録などを行うと共に、SAM からの利用履歴データ 308 に基づいてコンテンツプロバイダ 301 の決済請求権データを作成し、これをコンテンツプロバイダ 301 に送信してもよい。この場合には、コンテンツプロバイダ 301 は、自らの課金システムを電子決済用クリアリングハウス 961 として利用し、権利管理用クリアリングハウス 970 からの決済請求権データに基づいて決済を行う。

【0489】

また、本発明は、例えば、図 110 に示すように、コンテンツプロバイダ 301 内に、前述した権利管理用クリアリングハウス 970 および電子決済用クリアリングハウス 971 の機能を備えるようにしてもよい。

この場合には、コンテンツプロバイダ 301 は、自らの課金システムを電子決済用クリアリングハウス 961 として利用し、権利管理用クリアリングハウス 9

70において生成した決済請求権データに基づいて、決済機関91に対して自ら決済を行う。

【0490】

第2実施形態の第8変形例

上述した第2実施形態では、図59に示すEMDシステム300において、コンテンツプロバイダ301からサービスプロバイダ310に図5に示すフォーマットのセキュアコンテナ104を提供し、サービスプロバイダ310からユーザホームネットワーク303に図65に示すフォーマットのセキュアコンテナ304を配給する場合を例示した。

すなわち、上述した第2実施形態では、図5および図65に示すように、セキュアコンテナ104およびセキュアコンテナ304内に、それぞれ単数のコンテンツファイルCFと、当該コンテンツファイルCFに対応する単数のキーファイルKFを格納した場合を例示した。

本発明では、セキュアコンテナ104およびセキュアコンテナ304内に、それぞれ複数のコンテンツファイルCFと、当該複数のコンテンツファイルCFにそれぞれ対応する複数のキーファイルKFとを格納してもよい。

【0491】

図111は、本変形例において、図59に示すコンテンツプロバイダ301からサービスプロバイダ310に提供されるセキュアコンテナ104aのフォーマットを説明するための図である。

図111に示すように、セキュアコンテナ104aには、コンテンツファイルCF₁、CF₂、CF₃、キーファイルKF₁、KF₂、KF₃、公開鍵証明書データCER_{CP}、署名データSIG₂₀₀、CP、SIG₂₀₁、CP、SIG₂₀₂、CP、SIG₂₀₃、CP、SIG₂₀₄、CP、SIG₂₀₅、CP、SIG₁、ESCが格納されている。

ここで、署名データSIG₂₀₀、CP、SIG₂₀₁、CP、SIG₂₀₂、CP、SIG₂₀₃、CP、SIG₂₀₄、CP、SIG₂₀₅、CPは、コンテンツプロバイダ301において、それぞれコンテンツファイルCF₁、CF₂、CF₃、キーファイルKF₁、KF₂、KF₃に対してハッシュ値をとり、

コンテンツプロバイダ 301 の秘密鍵データ $K_{CP, S}$ を用いて生成される。

【0492】

コンテンツファイル CF_1 には、ヘッダ、メタデータ $Meta_1$ 、コンテンツデータ C_1 、A/V 伸長用ソフトウェア $Soft_1$ および電子透かし情報モジュール WM_1 が格納されている。

ここで、コンテンツデータ C_1 および A/V 伸長用ソフトウェア $Soft_1$ は、コンテンツ鍵データ Kc_1 を用いて暗号化されており、メタデータ $Meta_1$ および電子透かし情報モジュール WM_1 は必要に応じてコンテンツ鍵データ Kc_1 を用いて暗号化されている。

また、コンテンツデータ C_1 は、例えば、ATRAC3 方式で圧縮されている。A/V 伸長用ソフトウェア $Soft_1$ は、ATRAC3 方式の伸長用のソフトウェアである。

また、コンテンツファイル CF_1 のヘッダには、例えば、図 112 に示すようにキーファイル KF_1 およびコンテンツファイル CF_2 にリンクすることを示すディレクトリ構造データ DSD_1 が含まれている。

【0493】

コンテンツファイル CF_2 には、ヘッダ、メタデータ $Meta_2$ 、コンテンツデータ C_2 、A/V 伸長用ソフトウェア $Soft_2$ および電子透かし情報モジュール WM_2 が格納されている。

ここで、コンテンツデータ C_2 および A/V 伸長用ソフトウェア $Soft_2$ は、コンテンツ鍵データ Kc_2 を用いて暗号化されており、メタデータ $Meta_2$ および電子透かし情報モジュール WM_2 は必要に応じてコンテンツ鍵データ Kc_2 を用いて暗号化されている。

また、コンテンツデータ C_2 は、例えば、MPEG2 方式で圧縮されている。A/V 伸長用ソフトウェア $Soft_2$ は、MPEG2 方式の伸長用のソフトウェアである。

また、コンテンツファイル CF_2 のヘッダには、例えば、図 112 に示すように、キーファイル KF_2 およびコンテンツファイル CF_3 にリンクすることを示すディレクトリ構造データ DSD_2 が含まれている。

【0494】

コンテンツファイル CF_3 には、ヘッダ、メタデータ $Meta_3$ 、コンテンツデータ C_3 、A/V伸長用ソフトウェア $Soft_3$ および電子透かし情報モジュール WM_3 が格納されている。

ここで、コンテンツデータ C_3 および A/V伸長用ソフトウェア $Soft_3$ は、コンテンツ鍵データ Kc_3 を用いて暗号化されており、メタデータ $Meta_3$ および電子透かし情報モジュール WM_3 は必要に応じてコンテンツ鍵データ Kc_3 を用いて暗号化されている。

また、コンテンツデータ C_3 は、例えば、JPEG方式で圧縮されている。A/V伸長用ソフトウェア $Soft_3$ は、JPEG方式の伸長用のソフトウェアである。

また、コンテンツファイル CF_3 のヘッダには、例えば、図112に示すように、キーファイル KF_3 にリンクすることを示すディレクトリ構造データ DSD_3 が含まれている。

【0495】

キーファイル KF_1 には、ヘッダと、配信鍵データ $KD_1 \sim KD_3$ を用いて暗号化されたコンテンツ鍵データ Kc_1 、権利書データ 106_1 および SAMプログラム・ダウンロード・コンテナ SDC_1 と、署名データ SIG_{220} 、ESC とが格納されている。

【0496】

キーファイル KF_2 には、ヘッダと、配信鍵データ $KD_1 \sim KD_3$ を用いて暗号化されたコンテンツ鍵データ Kc_2 、権利書データ 106_2 および SAMプログラム・ダウンロード・コンテナ SDC_2 と、署名データ SIG_{221} 、ESC とが格納されている。

【0497】

キーファイル KF_3 には、ヘッダと、配信鍵データ $KD_1 \sim KD_3$ を用いて暗号化されたコンテンツ鍵データ Kc_3 、権利書データ 106_3 および SAMプログラム・ダウンロード・コンテナ SDC_3 と、署名データ SIG_{222} 、ESC とが格納されている。

【0498】

サービスプロバイダ310は、図112に示すセキュアコンテナ104aの配給を受けると、EMDサービスセンタ302の公開鍵データ $K_{ESC, P}$ を用いて公開鍵証明書データ CER_{CP} の正当性を確認した後に、当該公開鍵証明書データ CER_{CP} に格納された公開鍵データ $K_{CP, P}$ を用いて、署名データ $SIG_{200, CP}$ 、 $SIG_{201, CP}$ 、 $SIG_{202, CP}$ 、 $SIG_{203, CP}$ 、 $SIG_{204, CP}$ 、 $SIG_{205, CP}$ の正当性、すなわちコンテンツファイル CF_1 、 CF_2 、 CF_3 の作成者および送信者の正当性と、キーファイル KF_1 、 KF_2 、 KF_3 の送信者の正当性を確認する。

また、コンテンツプロバイダ301は、公開鍵データ $K_{ESC, P}$ を用いて、署名データ $SIG_{220, ESC}$ 、 $SIG_{221, ESC}$ 、 $SIG_{222, ESC}$ の正当性、キーファイル KF_1 、 KF_2 、 KF_3 の作成者の正当性を確認する。

【0499】

そして、サービスプロバイダ310は、コンテンツファイル CF_1 、 CF_2 、 CF_3 の販売価格を示すプライスタグデータ 312_1 、 312_2 、 312_3 を作成する。

また、サービスプロバイダ310は、秘密鍵データ $K_{SP, S}$ を用いて、プライスタグデータ 312_1 、 312_2 、 312_3 の署名データ $SIG_{220, SP}$ 、 $SIG_{221, SP}$ 、 $SIG_{222, SP}$ を作成する。

また、サービスプロバイダ310は、秘密鍵データ $K_{SP, S}$ を用いて、コンテンツファイル CF_1 、 CF_2 、 CF_3 、 KF_1 、 KF_2 、 KF_3 の署名データ $SIG_{210, SP}$ 、 $SIG_{211, SP}$ 、 $SIG_{212, SP}$ 、 $SIG_{213, SP}$ 、 $SIG_{214, SP}$ 、 $SIG_{215, SP}$ を作成する。

【0500】

次に、サービスプロバイダ310は、図114に示すセキュアコンテナ304aを作成する。

【0501】

サービスプロバイダ310は、図114に示すセキュアコンテナ304aをユ

ーザホームネットワーク 303 に配給する。

ユーザホームネットワーク 303 では、SAM305₁～305₄ において、セキュアコンテナ 304 a に格納された全ての署名データの正当性を確認した後に、コンテンツデータ C₁, C₂, C₃ についての権利処理を、ディレクトリ構造データ DSD₁～DSD₃ に示されるリンク状態に応じて、それぞれキーファイル KF₁, KF₂, KF₃ に基づいて行う。

【0502】

また、上述した第 8 変形例では、セキュアコンテナ 304 において、単数のサービスプロバイダ 310 から提供を受けた複数のコンテンツファイル CF₁₀₁, CF₁₀₂, CF₁₀₃ を単数のセキュアコンテナ 304 a に格納してユーザホームネットワーク 303 に配給する場合を例示したが、図 98 に示すように、複数のコンテンツプロバイダ 301 a, 301 b から提供を受けた複数のコンテンツファイル CF を、単数のセキュアコンテナに格納してユーザホームネットワーク 303 に配給してもよい。

【0503】

また、セキュアコンテナ 104, 304 内には、例えば、図 113 に示すように、ATRAC3 で圧縮された楽曲（音声）データを格納したコンテンツファイル CF₁、MP EG 2 で圧縮されたビデオクリップデータを格納したコンテンツファイル CF₂、J P E G で圧縮されたジャケット（静止画）データを格納したコンテンツファイル CF₃、テキスト形式の歌詞データを格納したコンテンツファイル CF₄ 並びにテキスト形式のライナーノーツデータを格納したコンテンツファイル CF₅ と、それぞれに対応したキーファイル KF₁, KF₂, KF₃, KF₄, KF₅ とを格納してもよい。

この場合にも、同様に、コンテンツファイル CF₁～CF₅ のディレクトリ構造データによって、コンテンツファイル CF₁～CF₅ 相互間のリンクと、コンテンツファイル CF₁～CF₅ とキーファイル KF₁～KF₅ との間のそれぞれのリンクとが確立される。

【0504】

なお、本実施形態におけるセキュアコンテナ内に複数のコンテンツデータを格

納する場合（コンポジット型の場合）のデータフォーマットの概念は、例えば、図 115 あるいは図 116 に示される。

【0505】

なお、図 111 に示すフォーマットは、前述した第 1 実施形態において、図 1 に示すコンテンツプロバイダ 101 からユーザホームネットワーク 103 にセキュアコンテナ 104 を送信する場合にも同様に適用できる。

【0506】

第 2 実施形態の第 9 変形例

上述した実施形態では、コンテンツファイル CF およびキーファイル KF をディレクトリ構造でセキュアコンテナ 104、304 に格納してコンテンツプロバイダ 301 からサービスプロバイダ 310、並びにサービスプロバイダ 310 から SAM305₁～305₄ に送信する場合を例示したが、コンテンツファイル CF およびキーファイル KF を、別々にコンテンツプロバイダ 301 からサービスプロバイダ 310、並びにサービスプロバイダ 310 から SAM305₁～305₄ に送信してもよい。

これには、例えば、以下に示す第 1 の手法と第 2 の手法とがある。

第 1 の手法では、図 117 に示すように、コンテンツプロバイダ 301 からサービスプロバイダ 310、並びにサービスプロバイダ 310 から SAM305₁～305₄ に、コンテンツファイル CF およびキーファイル KF を別々に送信する。

また、第 2 の手法では、図 118 に示すように、コンテンツプロバイダ 301 からサービスプロバイダ 310、並びにサービスプロバイダ 310 から SAM305₁～305₄ にコンテンツファイル CF を送信し、EMD サービスセンタ 302 から SAM305₁～305₄ にキーファイル KF を送信する。当該キーファイル KF の送信は、例えば、SAM305₁～305₄ のユーザが、コンテンツデータ C の購入形態を決定しようとするときに、EMD サービスセンタ 302 から SAM305₁～305₄ に送信される。

上述した第 1 の手法および第 2 の手法を採用する場合には、例えば、関連するコンテンツファイル CF 相互間と、コンテンツファイル CF とそれに対応するキ

ーファイルKFとの間を、コンテンツファイルCFおよびキーファイルKFの少なくとも一方のヘッダに格納されたハイパーリンクデータHLを用いてリンク関係を確立する。SAM105₁～105₄では、当該リンク関係に基づいて、コンテンツデータCの権利処理および利用を行う。

【0507】

また、上述した第2実施形態では、コンテンツデータCと、コンテンツ鍵データKcおよび権利書データ106などの鍵データとをそれぞれファイル形式にして、コンテンツプロバイダ301からサービスプロバイダ310、並びにサービスプロバイダ310からSAM305₁～305₄に送信する場合を例示したが、これらは、相互間でのリンク関係が確立できれば、必ずしもファイル形式にする必要はない。

例えば、図119に示すように、コンテンツデータC、メタデータMeata、A/V伸長用ソフトウェアSoft、電子透かし情報モジュールWM、キーファイルKF、プライスタグデータ312および、公開鍵証明書データCER_{CP}、CER_{SP}を別々に、コンテンツプロバイダ301およびEMDサービスセンタ302からSAM305₁～305₄に送信してもよい。

この場合には、図119に示すように、コンテンツデータC、メタデータMeata、A/V伸長用ソフトウェアSoft、電子透かし情報モジュールWM、キーファイルKF、プライスタグデータ312、公開鍵証明書データCER_{CP}、CER_{SP}が、ハイパーリンクデータHLによってリンクされる。

ここで、ハイパーリンクデータHLは、例えば、配信用鍵データKD₁～KD₆で暗号化されて送信される。

【0508】

なお、本変形例において、コンテンツファイルCFおよびキーファイルKFのフォーマットは、例えば、図5(A)、(B)に示すものが採用される。また、この場合に、コンテンツファイルCFおよびキーファイルKFと共に、それらの署名データSIG₆、CP、SIG₇、CPを送信することが好ましい。

【0509】

第2実施形態の第10変形例

上述した実施形態では、セキュアコンテナ 104 内において、コンテンツファイル CF およびキーファイル KF を別々に設けた場合を例示したが、例えば、図 120 に示すように、セキュアコンテナ 104, 304 内において、コンテンツファイル CF 内にキーファイル KF を格納するようにしてもよい。

この場合に、キーファイル KF を格納したコンテンツファイル CF に対して、コンテンツプロバイダ 301 の秘密鍵データ $K_{CP, S}$ による署名データ、並びにサービスプロバイダ 310 の秘密鍵データ $K_{SP, S}$ による署名データが付される。

第 2 実施形態の第 1 変形例

上述した実施形態では、コンテンツデータ C をコンテンツファイル CF に格納し、コンテンツ鍵データ Kc および権利書データ 106 をキーファイル KF 内に格納してコンテンツプロバイダ 301 からサービスプロバイダ 310、並びにサービスプロバイダ 310 から SAM305₁ などに送信する場合を例示したが、コンテンツデータ C、コンテンツ鍵データ Kc および権利書データ 106 の少なくとも一つをファイル形式を採用せずにコンテンツプロバイダ 301 からサービスプロバイダ 310、並びにサービスプロバイダ 310 から SAM305₁ などに、通信プロトコルに依存しない形式で送信してもよい。

【0510】

例えば、図 121 に示すように、コンテンツプロバイダ 301 において、コンテンツ鍵データ Kc で暗号化されたコンテンツデータ C と、暗号化されたコンテンツ鍵データ Kc および暗号化された権利書データ 106 などを含むキーファイル KF とを格納したセキュアコンテナ 104 s を作成し、セキュアコンテナ 104 s をサービスプロバイダ 310 に通信プロトコルに依存しない形式で送信する。そして、サービスプロバイダ 310 において、セキュアコンテナ 104 s に格納されたコンテンツデータ C およびキーファイル KF にプライスタグデータ 312 を加えてセキュアコンテナ 304 s を作成し、セキュアコンテナ 304 s を SAM305₁ などに通信プロトコルに依存しない形式で送信してもよい。

【0511】

また、図 122 に示すように、コンテンツプロバイダ 301 からサービスプロ

バイダ 310 に、コンテンツ鍵データ Kc で暗号化されたコンテンツデータ C と、暗号化されたコンテンツ鍵データ Kc および暗号化された権利書データ 106 などを含むキーファイル KF とを通信プロトコルに依存しない形式で個別に送信する。そして、サービスプロバイダ 310 から SAM305₁ などに、コンテンツデータ C、キーファイル KF およびプライスタグデータ 312 を通信プロトコルに依存しない形式で個別に送信する。すなわち、コンテンツデータ C をファイル形式にしないで、キーファイル KF と同一経路で送信する。

【0512】

また、図 123 に示すように、コンテンツプロバイダ 301 からサービスプロバイダ 310 に、コンテンツ鍵データ Kc で暗号化されたコンテンツデータ C を通信プロトコルに依存しない形式で送信し、サービスプロバイダ 310 から SAM305₁ などにコンテンツデータ C およびプライスタグデータ 312 を通信プロトコルに依存しない形式で送信する。また、暗号化されたコンテンツ鍵データ Kc および暗号化された権利書データ 106 などを含むキーファイル KF を EMD サービスセンタ 302 から SAM305₁ などに送信してもよい。すなわち、コンテンツデータ C をファイル形式にしないで、キーファイル KF と別経路で送信する。

【0513】

また、図 124 に示すように、コンテンツプロバイダ 301 からサービスプロバイダ 310 に、コンテンツ鍵データ Kc で暗号化されたコンテンツデータ C と、コンテンツ鍵データ Kc および権利書データ 106 とを、通信プロトコルに依存しない形式で送信する。また、サービスプロバイダ 310 から SAM305₁ などに、コンテンツデータ C、コンテンツ鍵データ Kc および権利書データ 106、並びにプライスタグデータ 312 を送信する。すなわち、コンテンツデータ C、コンテンツ鍵データ Kc、権利書データ 106 およびプライスタグデータ 312 をファイル形式にしないで、同一経路で送信する。

【0514】

また、図 125 に示すように、コンテンツプロバイダ 301 からサービスプロバイダ 310 に、コンテンツ鍵データ Kc で暗号化されたコンテンツデータ C を

、通信プロトコルに依存しない形式で送信する。そして、サービスプロバイダ 310 から SAM 305₁ などに、コンテンツデータ C およびプライスタグデータ 312 を、通信プロトコルに依存しない形式で送信する。また、EMD サービスセンタ 302 から SAM 305₁ などにコンテンツ鍵データ Kc および権利書データ 106 を送信する。。すなわち、コンテンツデータ C と、コンテンツ鍵データ Kc および権利書データ 106 とをファイル形式にしないで、別経路で送信する。

【0515】

第2実施形態の第12変形例

前述した図 59 に示す EMD システム 300 では、例えば、図 126 に示すように、ユーザホームネットワーク 303 がサービスプロバイダ 310 から受信したセキュアコンテナ 304 に応じたセキュアコンテナ 304A を、ユーザホームネットワーク 303a の SAM からの要求 S303a に応じて、ユーザホームネットワーク 303a に配給してもよい。

この場合には、ユーザホームネットワーク 303 の SAM が、前述した第 2 実施形態で説明したサービスプロバイダ 310 と同様の役割を果たすと考えることができる。

この場合に、ユーザホームネットワーク 303a の SAM は、独自にプライスタグデータ 312 を新たに設定できる。

そして、ユーザホームネットワーク 303a の SAM においてコンテンツデータ C の購入形態が決定され、それに応じた利用履歴データ 304a などがユーザホームネットワーク 303a の SAM から EMD サービスセンタ 302 に送信される。

EMD サービスセンタ 302 では、利用履歴データ 304a に基づいて、コンテンツプロバイダ 301、サービスプロバイダ 310、ユーザホームネットワーク 303 のユーザに、ユーザホームネットワーク 303a のユーザが支払った金銭を分配するための決済処理を行う。

【0516】

なお、本実施形態におけるセキュアコンテナのファイル包括大小関係は、図 1

27に示すように表現できる。

【0517】

第3実施形態

図128は本発明の第3実施形態のEMDシステムを説明するための図、図129は図128に示すEMDサービスセンタの機能ブロック図である。

図129において、前述した第1実施形態および第2実施形態で用いた符号と同じ符号を付した構成要素は、これらの実施形態で説明した同一符号の構成要素と同じである。

【0518】

本実施形態のEMDシステムでは、コンテンツプロバイダ301はEMDサービスセンタ302にマスタソース（コンテンツデータ）S111などを送り、EMDサービスセンタ302において例えば図5（A）に示すコンテンツファイルCFを作成する。

また、コンテンツプロバイダ301はEMDサービスセンタ302に、コンテンツデータS111のコンテンツID、コンテンツ鍵データKc、電子透かし管理情報（コンテンツデータに埋め込む電子透かし情報の内容）、コンテンツプロバイダ301の識別子CP_ID、コンテンツデータを提供するサービスプロバイダ310の識別子SP_ID、コンテンツデータの卸売価格SRPを送り、EMDサービスセンタ302において図5（B）に示すキーファイルKFを作成する。

また、EMDサービスセンタ302は、作成したコンテンツファイルCFをCFデータベース802aに格納し、個々のコンテンツファイルCFにグローバルユニークなコンテンツIDを付して、これらを一元的に管理する。また、EMDサービスセンタ302は、キーファイルKFをKFデータベース153aに格納し、これについてもコンテンツIDを用いて一元的に管理する。

【0519】

EMDサービスセンタ302における処理を図129を参照して説明する。

EMDサービスセンタ302は、コンテンツプロバイダ301から受け取ったマスタソースS111をコンテンツマスタソースデータベース801に格納する

次に、電子透かし情報付加部 112 において、コンテンツプロバイダ 301 から受け取った電子透かし管理情報が示す電子透かし情報を、コンテンツマスターデータベース 801 から読み出したマスターソース S111 に埋め込んでコンテンツデータ S112 を生成する。

次に、圧縮部 113 において、コンテンツデータ S112 を圧縮してコンテンツデータ S113 を生成する。

コンテンツデータ S112 は、伸長部 116 において伸長された後に、聴感検査部 123 において聴覚検査が行われ、必要であれば、電子透かし情報付加部 112 において電子透かし情報が再び埋め込まれる。

次に、暗号化部 114 において、コンテンツデータ S113 がコンテンツ鍵データ Kc を用いて暗号化されてコンテンツデータ S114 が生成される。

次に、CF 作成部 802 において、コンテンツデータ S114 などを格納した図 5 (A) に示すコンテンツファイル CF が作成され、コンテンツファイル CF が CF データベース 802a に格納される。

【0520】

また、EMD サービスセンタ 302 では、KF 作成部 153 において、図 5 (B) に示すキーファイル KF を作成し、キーファイル KF を KF データベース 153a に格納する。

【0521】

次に、セキュアコンテナ作成部 804 において、CF データベース 802a から読み出したコンテンツファイル CF と、KF データベース 153a から読み出したキーファイル KF とを格納したセキュアコンテナ 806 が作成され、セキュアコンテナ 806 がセキュアコンテナデータベース 805 に格納される。

その後、セキュアコンテナデータベース 805 が、サービスプロバイダ 310 によってアクセスされて、セキュアコンテナ 806 がサービスプロバイダ 310 に供給される。

【0522】

次に、サービスプロバイダ 310 は、セキュアコンテナ 806 に格納されたコ

ンテンツファイルCFおよびキーファイルKFと、コンテンツデータの販売価格を示すプライスタグデータ312とを格納したセキュアコンテナ807を作成する。

そして、サービスプロバイダ310は、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいはROM型などの記録媒体に記録してセキュアコンテナ807をユーザホームネットワーク303に配給する。

【0523】

ユーザホームネットワーク303では、オンラインの場合にはCAモジュール311を介してセキュアコンテナ807がSAM305₁などに提供され、SAM305₁などにおいて、キーファイルKFに格納されたコンテンツ鍵データKcおよび権利書データ106などが配信用鍵データKD₁~KD₂などを用いて復号され、復号された権利書データ106に基づいて、コンテンツファイルCFに格納されたコンテンツデータの購入形態などの取り扱いが決定される。

また、SAM305₁などにおいて、コンテンツデータの購入履歴などを示す利用履歴データ308が生成され、利用履歴データ308がEMDサービスセンタ302に送信される。

また、ユーザホームネットワーク303のSAM305₂から、ユーザホームネットワーク303aのSAM305₁₂にセキュアコンテナ807が配給された場合には、SAM305₁₂においてSAM305₂と同様の処理が行われ、SAM305₁₂からEMDサービスセンタ302に利用履歴データ308が送信される。

【0524】

なお、ユーザホームネットワーク303、303aにおけるセキュアコンテナ807に対しての処理は、前述した第1実施形態および第2実施形態におけるユーザホームネットワーク103、303における処理と同じである。

また、図128に示す例では、EMDサービスセンタ302からサービスプロバイダ310、並びにサービスプロバイダ310からユーザホームネットワーク303に、コンテンツファイルCFおよびキーファイルKFを格納したセキュアコンテナを送信する場合（イン・バンドの場合）を例示したが、コンテンツファ

イルCFおよびキーファイルKFを同一経路で別々に送信してもよい（アウト・オブ・バンドの場合）。

また、図130に示すように、EMDサービスセンタ302において作成したコンテンツファイルCFをサービスプロバイダ310に供給し、サービスプロバイダ310がコンテンツファイルCFをユーザホームネットワーク303に供給すると共に、EMDサービスセンタ302において作成したキーファイルKFをEMDサービスセンタ302からユーザホームネットワーク303、303aのSAM305₂、SAM305_{1 2}に供給してもよい。

【0525】

第4実施形態

図131は本発明の第4実施形態のEMDシステムを説明するための図である。

【0526】

本実施形態のEMDシステムでは、コンテンツプロバイダ301は例えば図5（A）に示すコンテンツファイルCFを作成し、これをEMDサービスセンタ302に送る。

また、コンテンツプロバイダ301はEMDサービスセンタ302に、コンテンツデータのコンテンツID、コンテンツ鍵データKc、電子透かし管理情報（コンテンツデータに埋め込む電子透かし情報の内容、並びに埋め込み位置情報）、コンテンツプロバイダ301の識別子CP_ID、コンテンツデータを提供するサービスプロバイダ310の識別子SP_ID、コンテンツデータの卸売価格SRPを送り、EMDサービスセンタ302において図5（B）に示すキーファイルKFを作成する。

また、EMDサービスセンタ302は、コンテンツファイルCFをCFデータベース802aに格納し、個々のコンテンツファイルCFにグローバルユニークなコンテンツIDを付して、これらを一元的に管理する。また、EMDサービスセンタ302は、作成したキーファイルKFをKFデータベース153aに格納し、これについてもコンテンツIDを用いて一元的に管理する。

【0527】

また、EMDサービスセンタ302では、CFデータベース802aから読み出したコンテンツファイルCFと、KFデータベース153aから読み出したキーファイルKFとを格納したセキュアコンテナ806が作成され、セキュアコンテナ806がセキュアコンテナデータベースに格納される。

その後、セキュアコンテナデータベースが、サービスプロバイダ310によってアクセスされて、セキュアコンテナ806がサービスプロバイダ310に供給される。

【0528】

次に、サービスプロバイダ310は、セキュアコンテナ806に格納されたコンテンツファイルCFおよびキーファイルKFと、コンテンツデータの販売価格を示すプライスタグデータ312とを格納したセキュアコンテナ807を作成する。

そして、サービスプロバイダ310は、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいはROM型などの記録媒体に記録してセキュアコンテナ807をユーザホームネットワーク303に配給する。

【0529】

ユーザホームネットワーク303では、オンラインの場合にはCAモジュール311を介してセキュアコンテナ807がSAM305₁などに提供され、SAM305₁などにおいて、キーファイルKFに格納されたコンテンツ鍵データKcおよび権利書データ106などが配信用鍵データKD₁~KD₃などを用いて復号され、復号された権利書データ106に基づいて、コンテンツファイルCFに格納されたコンテンツデータの購入形態などの取り扱いが決定される。

また、SAM305₁などにおいて、コンテンツデータの購入履歴などを示す利用履歴データ308が生成され、利用履歴データ308がEMDサービスセンタ302に送信される。

また、ユーザホームネットワーク303のSAM305₂から、ユーザホームネットワーク303aのSAM305₁₂にセキュアコンテナ807が配給された場合には、SAM305₁₂においてSAM305₂と同様の処理が行われ、SAM305₁₂からEMDサービスセンタ302に利用履歴データ308が送

信される。

【0530】

なお、ユーザホームネットワーク303、303aにおけるセキュアコンテナ807に対しての処理は、前述した第1実施形態および第2実施形態におけるユーザホームネットワーク103、303における処理と同じである。

また、図131に示す例では、EMDサービスセンタ302からサービスプロバイダ310、並びにサービスプロバイダ310からユーザホームネットワーク303に、コンテンツファイルCFおよびキーファイルKFを格納したセキュアコンテナを送信する場合（イン・バンドの場合）を例示したが、コンテンツファイルCFおよびキーファイルKFを同一経路で別々に送信してもよい（アウト・バンドの場合）。

また、図132に示すように、コンテンツファイルCFをEMDサービスセンタ302からサービスプロバイダ310に供給し、サービスプロバイダ310がコンテンツファイルCFをユーザホームネットワーク303に供給すると共に、EMDサービスセンタ302において作成したキーファイルKFをEMDサービスセンタ302からユーザホームネットワーク303、303aのSAM305₂、SAM305₁₂に供給してもよい。

【0531】

第5実施形態

図133は本発明の第5実施形態のEMDシステムを説明するための図である。

【0532】

本実施形態のEMDシステムでは、コンテンツプロバイダ301は例えば図5(A)に示すコンテンツファイルCFを作成する。

また、コンテンツプロバイダ301はEMDサービスセンタ302に、コンテンツデータのコンテンツID、コンテンツ鍵データKc、電子透かし管理情報（コンテンツデータに埋め込む電子透かし情報の内容、並びに埋め込み位置情報）、コンテンツプロバイダ301の識別子CP_ID、コンテンツデータを提供するサービスプロバイダ310の識別子SP_ID、コンテンツデータの卸売価格

SRPを送り、EMDサービスセンタ302において図5（B）に示すキーファイルKFを作成する。

EMDサービスセンタ302は、作成したキーファイルKFをコンテンツプロバイダ301に送る。

また、EMDサービスセンタ302は、KFデータベース153aにキーファイルKFを格納し、個々のコンテンツデータに割り当てられたコンテンツIDを用いてキーファイルKFを一元的に管理する。このとき、コンテンツIDは、例えば、EMDサービスセンタ302によって作成され、複数のコンテンツプロバイダ301が提供するコンテンツデータの全てを対象としてグローバルユニークに決定される。

【0533】

次に、コンテンツプロバイダ301において、作成したコンテンツファイルCFと、EMDサービスセンタ302から受けたキーファイルKFとを格納したセキュアコンテナ821が作成され、セキュアコンテナ821が共通データベース820に格納される。

共通データベース820において、複数のコンテンツプロバイダ301が提供したセキュアコンテナ821が、コンテンツIDを用いて一元的に管理される。

【0534】

サービスプロバイダ310は、例えば、コンテンツIDを用いて共通データベース820をブランジング（検索）して、所望のセキュアコンテナ821を共通データベース820から受けて、セキュアコンテナ821に、コンテンツの販売価格を示すプライスタグデータ312などをさらに格納したセキュアコンテナ822を作成し、セキュアコンテナ822をユーザホームネットワーク303に配給する。

【0535】

ユーザホームネットワーク303では、オンラインの場合にはCAモジュール311を介してセキュアコンテナ822がSAM305₁などに提供され、SAM305₁などにおいて、キーファイルKFに格納されたコンテンツ鍵データKcおよび権利書データ106などが配信用鍵データKD₁～KD₂などを用い

て復号され、復号された権利書データ 106 に基づいて、コンテンツファイル C F に格納されたコンテンツデータの購入形態などの取り扱いが決定される。

また、SAM305₁ などにおいて、コンテンツデータの購入履歴などを示す利用履歴データ 308 が生成され、利用履歴データ 308 が EMD サービスセンタ 302 に送信される。

また、ユーザホームネットワーク 303 の SAM305₂ から、ユーザホームネットワーク 303 a の SAM305₁₂ にセキュアコンテナ 822 が配給された場合には、SAM305₁₂ において SAM305₂ と同様の処理が行われ、SAM305₁₂ から EMD サービスセンタ 302 に利用履歴データ 308 が送信される。

【0536】

なお、ユーザホームネットワーク 303、303 a におけるセキュアコンテナ 807 に対しての処理は、前述した第 1 実施形態および第 2 実施形態におけるユーザホームネットワーク 103、303 における処理と同じである。

また、図 133 に示す例では、コンテンツプロバイダ 301 から共通データベース 820、共通データベース 820 からサービスプロバイダ 310、並びにサービスプロバイダ 310 からユーザホームネットワーク 303 に、コンテンツファイル C F およびキーファイル K F を格納したセキュアコンテナを送る場合（イン・バンドの場合）を例示したが、コンテンツファイル C F およびキーファイル K F を同一経路で別々に送信してもよい（アウト・オブ・バンドの場合）。

また、図 134 に示すように、コンテンツプロバイダ 301 から共通データベース 820 にコンテンツファイル C F を格納し、サービスプロバイダ 310 が共通データベース 820 からコンテンツファイル C F を得ると共に、EMD サービスセンタ 302 からサービスプロバイダ 310 にキーファイル K F を送るようにしてもよい。この場合には、サービスプロバイダ 310 は、共通データベース 820 から得たコンテンツファイル C F と、EMD サービスセンタ 302 から得たキーファイル K F と、プライスタグデータ 312 とを格納してセキュアコンテナ 822 を作成する。

共通データベース 820 は、複数のコンテンツプロバイダ 301 が提供するコ

ンテンツデータに対してグローバルユニークに付されたコンテンツIDを用いて、コンテンツファイルCFを一元的に管理する。

【0537】

また、図135に示すように、EMDサービスセンタ302が作成したキーファイルKFを、ユーザホームネットワーク303、303aのSAM305₁、305₁₂などに送るようにしてもよい。この場合には、サービスプロバイダ310は、コンテンツファイルCFをユーザホームネットワーク303に配給する。プライスタグデータ312は、サービスプロバイダ310がユーザホームネットワーク303に配給してもよいし、EMDサービスセンタ302がユーザホームネットワーク303、303aに配給してもよい。

【0538】

第6実施形態

図136は本発明の第6実施形態のEMDシステムを説明するための図である

【0539】

本実施形態のEMDシステムは、前述した図133に示すEMDシステムと比較すると、複数のEMDサービスセンタ302を有し、コンテンツプロバイダ301がそれぞれ対応するEMDサービスセンタ302との間で課金処理などを行うことを特徴としている点が異なり、それ以外の点は略同じである。

コンテンツプロバイダ301は例えば図5(A)に示すコンテンツファイルCFを作成する。

また、コンテンツプロバイダ301は、複数のEMDサービスセンタ302のうち自らが選択した（あるいは予め決められた）一のEMDサービスセンタ302に、コンテンツデータのコンテンツID、コンテンツ鍵データKc、電子透かし管理情報（コンテンツデータに埋め込む電子透かし情報の内容、並びに埋め込み位置情報）、コンテンツプロバイダ301の識別子CP_ID、コンテンツデータを提供するサービスプロバイダ310の識別子SP_ID、コンテンツデータの卸売価格SRPを送り、EMDサービスセンタ302において図5(B)に示すキーファイルKFを作成する。

EMDサービスセンタ302は、作成したキーファイルKFを、対応するコン

テンツプロバイダ 301 に送る。

また、EMD サービスセンタ 302 は、KF データベース 153a にキーファイル KF を格納し、個々のコンテンツデータに割り当てられたコンテンツ ID を用いてキーファイル KF を一元的に管理する。このとき、コンテンツ ID は、例えば、EMD サービスセンタ 302 によって作成され、共通データベース 830 に格納される全てのセキュアコンテナ 831 に対応するコンテンツデータを対象としてグローバルユニークに決定される。

【0540】

次に、コンテンツプロバイダ 301 において、作成したコンテンツファイル CF と、EMD サービスセンタ 302 から受けたキーファイル KF とを格納したセキュアコンテナ 831 が作成され、セキュアコンテナ 831 が共通データベース 820 に格納される。

共通データベース 830 において、複数のコンテンツプロバイダ 301 が提供したセキュアコンテナ 831 が、コンテンツ ID を用いて一元的に管理される。

【0541】

サービスプロバイダ 310 は、例えば、コンテンツ ID を用いて共通データベース 820 をブランジング（検索）して、所望のセキュアコンテナ 831 を共通データベース 820 から受けて、セキュアコンテナ 831 に、コンテンツの販売価格を示すプライスタグデータ 312 などをさらに格納したセキュアコンテナ 832 を作成し、セキュアコンテナ 832 をユーザホームネットワーク 303 に配給する。

【0542】

ユーザホームネットワーク 303 では、オンラインの場合には CA モジュール 311 を介してセキュアコンテナ 832 が SAM 305₁ などに提供され、SAM 305₁ などにおいて、キーファイル KF に格納されたコンテンツ鍵データ Kc および権利書データ 106 などが配信用鍵データ KD₁ ~ KD₃ などを用いて復号され、復号された権利書データ 106 に基づいて、コンテンツファイル CF に格納されたコンテンツデータの購入形態などの取り扱いが決定される。

また、SAM 305₁ などにおいて、コンテンツデータの購入履歴などを示す

利用履歴データ 308 が生成され、利用履歴データ 308 が EMD サービスセンタ 302 に送信される。

また、ユーザホームネットワーク 303 の SAM305₂ から、ユーザホームネットワーク 303 a の SAM305₁₂ にセキュアコンテナ 832 が配給された場合には、SAM305₁₂ において SAM305₂ と同様の処理が行われ、SAM305₁₂ から EMD サービスセンタ 302 に利用履歴データ 308 が送信される。

【0543】

なお、ユーザホームネットワーク 303, 303 a におけるセキュアコンテナ 807 に対しての処理は、前述した第 1 実施形態および第 2 実施形態におけるユーザホームネットワーク 103, 303 における処理と同じである。

また、図 136 に示す例では、コンテンツプロバイダ 301 から共通データベース 830、共通データベース 830 からサービスプロバイダ 310、並びにサービスプロバイダ 310 からユーザホームネットワーク 303 に、コンテンツファイル CF およびキーファイル KF を格納したセキュアコンテナを送る場合（イン・バンドの場合）を例示したが、コンテンツファイル CF およびキーファイル KF を同一経路で別々に送信してもよい（アウト・オブ・バンドの場合）。

また、図 137 に示すように、コンテンツプロバイダ 301 から共通データベース 830 にコンテンツファイル CF を格納し、サービスプロバイダ 310 が共通データベース 820 からコンテンツファイル CF を得ると共に、EMD サービスセンタ 302 からサービスプロバイダ 310 にキーファイル KF を送るようにしてもよい。このとき、サービスプロバイダ 310 が得たコンテンツファイル CF を作成したコンテンツプロバイダ 301 に対応する EMD サービスセンタ 302 からサービスプロバイダ 310 にキーファイル KF が送られる。

【0544】

サービスプロバイダ 310 は、共通データベース 830 から得たコンテンツファイル CF と、EMD サービスセンタ 302 から得たキーファイル KF と、プライスタグデータ 312 とを格納してセキュアコンテナ 832 を作成する。

共通データベース 830 は、複数のコンテンツプロバイダ 301 が提供するコ

ンテンツデータに対してグローバルユニークに付されたコンテンツIDを用いて、コンテンツファイルCFを一元的に管理する。

【0545】

また、図138に示すように、EMDサービスセンタ302が作成したキーファイルKFを、ユーザホームネットワーク303、303aのSAM305₁、305₁₂などに送るようにしてもよい。このときも、SAM305₁、305₁₂などに提供されたコンテンツファイルCFを作成したコンテンツプロバイダ301に対応するEMDサービスセンタ302からSAM305₁、305₁₂などにキーファイルKFが送られる。

また、サービスプロバイダ310は、コンテンツファイルCFをユーザホームネットワーク303に配給する。プライスタグデータ312は、サービスプロバイダ310がユーザホームネットワーク303に配給してもよいし、EMDサービスセンタ302がユーザホームネットワーク303、303aに配給してもよい。

【0546】

第7実施形態

図139は本発明の第7実施形態のEMDシステムを説明するための図である。

【0547】

本実施形態のEMDシステムは、前述した図136に示すEMDシステムと比較すると、コンテンツプロバイダ301からEMDサービスセンタ302にコンテンツデータのマスソースS111を送り、EMDサービスセンタ302においてコンテンツファイルCFを作成する点が異なり、それ以外の点は略同じである。

コンテンツプロバイダ301は、コンテンツデータのマスソースS111を複数のEMDサービスセンタ302のうち自らが選択した（あるいは予め決められた）一のEMDサービスセンタ302に送り、EMDサービスセンタ302において、図5（A）に示すコンテンツファイルCFを作成する。

EMDサービスセンタ302は、作成したコンテンツファイルCFを対応する

コンテンツプロバイダ 301 に送る。

【0548】

また、コンテンツプロバイダ 301 は、上記一の対応する EMD サービスセンタ 302 に、コンテンツデータのコンテンツ ID、コンテンツ鍵データ Kc、電子透かし管理情報（コンテンツデータに埋め込む電子透かし情報の内容）、コンテンツプロバイダ 301 の識別子 CP_ID、コンテンツデータを提供するサービスプロバイダ 310 の識別子 SP_ID、コンテンツデータの卸売価格 SRP を送り、EMD サービスセンタ 302 において図 5（B）に示すキーファイル KF を作成する。

EMD サービスセンタ 302 は、作成したキーファイル KF を、対応するコンテンツプロバイダ 301 に送る。

また、EMD サービスセンタ 302 は、CF データベース 802a にコンテンツファイル CF を格納し、KF データベース 153a にキーファイル KF を格納し、個々のコンテンツデータに割り当てられたコンテンツ ID を用いてコンテンツファイル CF およびキーファイル KF を一元的に管理する。このとき、コンテンツ ID は、例えば、EMD サービスセンタ 302 によって作成され、共通データベース 840 に格納される全てのセキュアコンテナ 831 に対応するコンテンツデータを対象としてグローバルユニークに決定される。

【0549】

次に、コンテンツプロバイダ 301 において、対応する EMD サービスセンタ 302 から受けたコンテンツファイル CF およびキーファイル KF とを格納したセキュアコンテナ 841 が作成され、セキュアコンテナ 841 が共通データベース 840 に格納される。

共通データベース 840 において、複数のコンテンツプロバイダ 301 が提供したセキュアコンテナ 841 が、コンテンツ ID を用いて一元的に管理される。

【0550】

サービスプロバイダ 310 は、例えば、コンテンツ ID を用いて共通データベース 840 をブランジング（検索）して、所望のセキュアコンテナ 841 を共通データベース 840 から受けて、セキュアコンテナ 841 に、コンテンツの販売

価格を示すプライスタグデータ 312などをさらに格納したセキュアコンテナ 842を作成し、セキュアコンテナ 842をユーザホームネットワーク 303に配給する。

【0551】

ユーザホームネットワーク 303では、オンラインの場合にはCAモジュール 311を介してセキュアコンテナ 842がSAM 305₁などに提供され、SAM 305₁などにおいて、キーファイルKFに格納されたコンテンツ鍵データ Kcおよび権利書データ 106などが配信用鍵データ KD₁~KD₃などを用いて復号され、復号された権利書データ 106に基づいて、コンテンツファイルCFに格納されたコンテンツデータの購入形態などの取り扱いが決定される。

また、SAM 305₁などにおいて、コンテンツデータの購入履歴などを示す利用履歴データ 308が生成され、利用履歴データ 308がEMDサービスセンタ 302に送信される。

また、ユーザホームネットワーク 303のSAM 305₂から、ユーザホームネットワーク 303aのSAM 305₁₂にセキュアコンテナ 832が配給された場合には、SAM 305₁₂においてSAM 305₂と同様の処理が行われ、SAM 305₁₂からEMDサービスセンタ 302に利用履歴データ 308が送信される。

【0552】

なお、ユーザホームネットワーク 303, 303aにおけるセキュアコンテナ 807に対しての処理は、前述した第1実施形態および第2実施形態におけるユーザホームネットワーク 103, 303における処理と同じである。

また、図139に示す例では、コンテンツプロバイダ 301から共通データベース 840、共通データベース 840からサービスプロバイダ 310、並びにサービスプロバイダ 310からユーザホームネットワーク 303に、コンテンツファイルCFおよびキーファイルKFを格納したセキュアコンテナを送る場合（イン・バンドの場合）を例示したが、コンテンツファイルCFおよびキーファイルKFを同一経路で別々に送信してもよい（アウト・オブ・バンドの場合）。

また、図140に示すように、コンテンツプロバイダ 301から共通データベ

ース 830 にコンテンツファイル CF を格納し、サービスプロバイダ 310 が共通データベース 820 からコンテンツファイル CF を得ると共に、EMD サービスセンタ 302 からサービスプロバイダ 310 にキーファイル KF を送るようにしてもよい。このとき、サービスプロバイダ 310 が得たコンテンツファイル CF を作成したコンテンツプロバイダ 301 に対応する EMD サービスセンタ 302 からサービスプロバイダ 310 にキーファイル KF が送られる。

【0553】

サービスプロバイダ 310 は、共通データベース 840 から得たコンテンツファイル CF と、EMD サービスセンタ 302 から得たキーファイル KF と、プライスタグデータ 312 とを格納してセキュアコンテナ 842 を作成する。

共通データベース 830 は、複数のコンテンツプロバイダ 301 が提供するコンテンツデータに対してグローバルユニークに付されたコンテンツ ID を用いて、コンテンツファイル CF を一元的に管理する。

【0554】

また、図 141 に示すように、EMD サービスセンタ 302 が作成したキーファイル KF を、ユーザホームネットワーク 303、303a の SAM305₁、305₁₂ などに送るようにしてもよい。このときも、SAM305₁、305₁₂ などに提供されたコンテンツファイル CF を作成したコンテンツプロバイダ 301 に対応する EMD サービスセンタ 302 から SAM305₁、305₁₂ などにキーファイル KF が送られる。

また、サービスプロバイダ 310 は、コンテンツファイル CF をユーザホームネットワーク 303 に配給する。プライスタグデータ 312 は、サービスプロバイダ 310 がユーザホームネットワーク 303 に配給してもよいし、EMD サービスセンタ 302 がユーザホームネットワーク 303、303a に配給してもよい。

【0555】

第 8 実施形態

図 142 は、本発明の第 8 実施形態の EMD システムを説明するための図である。

本実施形態のEMDシステムでは、例えば、コンテンツプロバイダ301からEMDサービスセンタ302に提供されたマスタソースを用いてEMDサービスセンタ302が作成した図5（A）に示すコンテンツファイルCF、あるいはコンテンツプロバイダ301が作成してEMDサービスセンタ302に提供した図5（A）に示すコンテンツファイルCFと、EMDサービスセンタ302が作成した図5（B）に示すキーファイルKFとが、EMDサービスセンタ302によってサービスプロバイダ310を介して、あるいは直接的にユーザホームネットワーク303のSAM305₁に配信される。

ここで、サービスプロバイダ310は、コンテンツファイルCFの販売価格を示すプライスタグデータ312をユーザホームネットワーク303に送ると共に、プライスタグデータ312をEMDサービスセンタ302に登録して権威化する。

また、サービスプロバイダ310は、自らを、配信事業者としてEMDサービスセンタ302に登録する。

【0556】

本実施形態のEMDシステムでは、ユーザホームネットワーク303の例えばSAM305₁が、サービスプロバイダ310あるいはEMDサービスセンタ302から得たコンテンツファイルCFおよびキーファイルKFを、ユーザホームネットワーク303内のSAM305₂および／またはユーザホームネットワーク303a内のSAM305₁₂などに配信する配信事業者となる。

但し、この場合に、例えば、EMDサービスセンタ302は、SAM305₁がコンテンツファイルCFに格納されたコンテンツデータCを購入した後に、当該購入したコンテンツデータCを、何らかの販売マージンを加えて販売（再配付）して利益を上げることを禁止する。

本実施形態のEMDシステムでは、購入形態が未決定のコンテンツデータC、あるいは、購入形態として再生課金が決定されているコンテンツデータCを、販売利益マージンをとらずに再配付することを条件に、SAM305₁がコンテンツデータCを他のSAMに複製することを許可する。なお、これを機器間再配布と呼ぶ。

また、本実施形態のEMDシステムでは、SAM305₁がサービスプロバイダ310から配給を受けたコンテンツファイルCF（あるいはセキュアコンテナ）に関しては、販売利益マージンをとらない形態での機器間売買は許可される。

また、本実施形態では、SAM305₁が、販売利益マージンをとる形態でのコンテンツデータCの販売（配信）を行う場合には、SAM305₁はEMDサービスセンタ302に自らを配信事業者として登録して許諾を受けると共に、コンテンツデータCの販売価格を示すプライスタグデータ312をEMDサービスセンタ302に登録する。そして、SAM305₁は、サービスプロバイダ310を介さずに、EMDサービスセンタ302内のCFデータベース802aおよびKFデータベース153aから直接的にコンテンツファイルCFおよびキーファイルKFの配給を受ける。

【0557】

第9実施形態

図143は、本発明の第9実施形態のEMDシステムを説明するための図である。

本実施形態のEMDシステムでは、コンテンツプロバイダ301のそれぞれが、コンテンツプロバイダとしての役割に加えて、EMDサービスセンタ302としての役割を果たすことを特徴としてる。

おの場合に、複数のコンテンツプロバイダ301がある場合に、それぞれのコンテンツプロバイダ301は、それぞれのEMDサービスセンタ302としての役割を持つ。

コンテンツプロバイダ301は、コンテンツファイルCFおよびキーファイルKFを格納したセキュアコンテナ851をサービスプロバイダ310に配信する。

サービスプロバイダ310は、セキュアコンテナ851が格納したコンテンツファイルCF、キーファイルKFに、さらにプライスタグデータ312を加えてセキュアコンテナ852を作成し、これをユーザホームネットワーク303に配信する。

ユーザホームネットワーク303、303aでは、キーファイルKF内に格納

された権利書データ 106 に基づいてコンテンツファイル CF の購入形態などを決定し、それに応じた利用履歴データ 308 を作成し、これをコンテンツプロバイダ 301 内の EMD サービスセンタ 302 に送信する。

このとき、利用履歴データ 308 は、コンテンツプロバイダ 301 毎に作成される。

コンテンツプロバイダ 301 の EMD サービスセンタ 302 は、利用履歴データ 308 に基づいて、SAM 305₁, 305₁₂ のユーザが支払った利益を、自らと対応するサービスプロバイダ 310 との間で分配する。

また、ユーザホームネットワーク 303 の CA モジュール 311 から、配信サービスに関しての履歴データが対応するサービスプロバイダ 310 に送られ、サービスプロバイダ 310 において配信サービスに対しての課金処理が行われる。

【0558】

本発明は上述した実施形態には限定されない。

上述した実施形態では、コンテンツデータとしてオーディオデータを用いる場合を例示したが、コンテンツデータとして、ビデオデータ、オーディオ・ビデオデータ、テキストデータおよびコンピュータプログラムなどを用いてもよい。

また、上述した実施形態では、EMD サービスセンタ 102, 302 において、キーファイル KF を作成する場合を例示したが、コンテンツプロバイダ 101, 301 においてキーファイル KF を作成することも可能である。

この場合に、図 7 に対応するキーファイル KF のフォーマットは、図 144 に示すようになる。図 144 に示すように、当該キーファイル KF は、コンテンツプロバイダ 101, 301 の秘密鍵データ K_{CP}, S を用いて作成された署名データが用いられる点を除いて、図 7 に示すキーファイル KF と基本的に同じ情報を有している。

【0559】

また、上述した実施形態では、ユーザホームネットワーク 103, 303 から EMD サービスセンタ 102, 302 に、利用制御状態データ 166 をリアルタイムで送信する場合を例示したが、利用制御状態データ 166 をコンテンツプロバイダ 101, 301 および／またはサービスプロバイダ 310 に送信するよう

にしてもよい。これにより、コンテンツプロバイダ 101, 301 およびサービスプロバイダ 310 は、自らが提供および配給したコンテンツの購入状況を即座に把握でき、その後のサービスに反映できる。

【0560】

以下、上述した本実施形態の EMD システムによる効果を、従来技術およびその問題点を述べながら再び説明する。

デジタル放送（データ放送）、インターネットなどのデジタルネットワークが発達していない時代に、デジタルコンテンツ（コンテンツデータ）を流用させる手段として使用されていた ROM 型記録媒体では、デジタルコンテンツを非暗号化の状態で記録して流用させていた。デジタルネットワークが発達していない時代では、これらのコンテンツの著作権保護をおこなうのは、ユーザホームネットワーク上でのユーザによるカジュアルコピーを防ぐ方法を考えるだけで良かった。

【0561】

しかしながら、デジタルネットワークが発達してきた昨今では、非暗号化コンテンツが搭載されている ROM 型記録媒体を一般市民が、いつ、どこでも、自由に入手することができるために、各自がこれらを購入し、圧縮してネットワークにアップロードすることが簡単にできてしまう。特にインターネットは世界中につながっているネットワークなので、非暗号化コンテンツを無料でインターネット上にアップロードし、市民はそれを無料で自分の個人端末にダウンロードすることが可能となってしまう、コンテンツの権利者（コンテンツプロバイダ）の著作権を著しく侵害する可能性が出てきている。

【0562】

また、非暗号化の状態でアップロードせず、自らが、そのコンテンツに対し、独自方式の電子透かし情報を埋め込み、暗号化をおこなうことで独自方式の課金機能を備え、インターネット上で著作権の許可なしに、目の届かないところで勝手に、デジタルコンテンツの販売をおこなうことも可能となっている。このときは、売り上げの一部がコンテンツの権利者に還元されないので、コンテンツの権利者（コンテンツプロバイダ）の著作権を著しく侵害することになる。

また、著作権者の許諾を得て、売り上げの一部をコンテンツの権利者（コンテンツプロバイダ）に還元する契約を権利者側と事前におこなうことで、これらのデジタルコンテンツを配信して利益が得られる配信サービスをおこなうことが可能になるが、基本的にコンテンツプロバイダは、こういったコンテンツの2次利用による流通体系をあまり好ましく思っていない。コンテンツの2次利用によるビジネスとは、たとえばレンタルビジネス、中古販売などが相当する。

2次利用による配信サービスが登場する時は、必ず著作権侵害の問題が起こり、サービス自体を軌道に載せるまで時間がかかる。コンテンツプロバイダと事前契約をおこなうことなしに、まず配信サービスを始めてしまい、著作権侵害ということで問題になってから、権利者側への利益分配なり著作権保護が考慮され配信サービスとしての許諾が得られる。レンタルCD、レンタルビデオが相当する。ゲームソフトの中古販売などは深刻な問題である。現在ゲームソフトの中古販売ビジネスでは、売り上げの利益の一部がコンテンツの権利者側に還元されないもので、権利者側は裁判で告訴しているが却下され、権利者側にとって非常に酷になっている。新作ソフトの半額以下で大量に販売されるので、ユーザからしても魅力がある市場で、新作ソフトの売り上げにも影響を及ぼす。

【0563】

コンテンツの2次利用というのは、本来コンテンツの権利者がROM型記録媒体を流通手段とし、そのデジタルコンテンツ記録済のROM型記録媒体を商品として流通させて利益を得ている訳で、それらを購入したユーザによって、その商品をさらに流通させることで、購入したユーザが利益を得ることは、たとえ利益の一部が還元されたとしても、（コンテンツプロバイダ）権利者側の立場からするとあまり好ましく思わない。映画コンテンツなどは、録音権／領布権というのがコンテンツの権利者側に法律で保障されており、権利者が世に流通させたコンテンツを、それを購入した時点で、その購入ユーザの手元からは流通しないことを前提としている。ゲームソフトの権利者団体は、この領布権の権利をゲームソフトにも利用し、2次利用ビジネスの抑制を裁判で訴えている。

【0564】

コンテンツの権利者は、自分が著作権を持っているデジタルコンテンツについ

ては、それを流用させる流通業者を管理下においておきたい（誰に流通させているか、を知っておきたい）。自分が著作権を持っているデジタルコンテンツを流通させて配信サービスをおこない利益を得ることを希望している配信事業者がいる場合は、コンテンツの権利者から直接デジタルコンテンツを渡せるようなシステムが望ましい。

なお、ここで述べている流通業者とは、デジタルコンテンツの対価に、さらに何%かの利益マージンを徴収することで利益を得る業者を指す。

デジタルコンテンツを他機器／記録媒体へ渡すときに利益マージンを徴収する場合、そのコンテンツ売買セッション配信サービスとして定義し、利益マージンを徴収しない場合を機器間再配付として定義し、これは超流通の原理により合法である。

コンテンツプロバイダが流通させた非暗号化コンテンツが記録されているROM型記録媒体からサービスプロバイダが、自分の配信サービス用コンテンツをオーサリングし、配信サービスをおこなう現状のデジタルコンテンツのネットワーク流通管理システムにおいて、コンテンツプロバイダが所有している一つのデジタルコンテンツが複数のサービスプロバイダによって配信される状況を考えると、同一コンテンツであるにも関わらず、各々のサービスプロバイダが採用するCAモジュール／電子決済ツールにて権利処理がおこなわれるようにオーサリングされるため、使用される暗号鍵（コンテンツ鍵データ）、コンテンツの使用許諾条件（権利書データ）のフォーマットが各サービスプロバイダによって各々異なり、ユーザホームネットワーク上で共通の権利処理ルールを提供することができない。こういった場合では、CAモジュール／電子決済ツールで利用する鍵データ類をすべてネットワーク機器のCAモジュール／電子決済ツールで清算し、あとはSCMSのルールに準拠することでユーザホームネットワーク上での共通の権利処理ルールを実現している。

また、CAモジュール／電子決済ツールの鍵で暗号化されたコンテンツと鍵データを、そのままネットワーク機器を通過してユーザホームネットワークバス（IEEE1394など。）を経由してストレージ機器の記録媒体に記録し、1394バス上につながる機器から遠隔的にネットワーク機器を経由してコンテンツ

の購入、決済処理ができたとしても、暗号化コンテンツを復号するためのデスクランブラがネットワーク機器に存在するので、結局再生時にネットワーク機器まで、コンテンツと鍵データを戻さないと再生できない（ネットワークCA）。

【0565】

上述したように、現在までに世の中に広く流通している非暗号化コンテンツが記録されているROM型記録媒体の存在が、現状のデジタルコンテンツネットワーク配信サービスにとって問題の根源となっている。デジタルコンテンツのコンテンツ形態が、コンテンツプロバイダ以外の第3者によって作成される可能性を持っており、さらに、ユーザに対して、そのコンテンツを販売した人が、その対価を入手するシステムであるため、コンテンツの2次利用などコンテンツプロバイダの利益が不当に損なわれる可能性がある。また、オーサリングしたデジタルコンテンツの流通管理をコンテンツプロバイダが厳密におこなっていないため、自分が著作権を持っているデジタルコンテンツが稼ぎ出す全利益、およびそこから自分の利益分が還元されているかどうかを監視することが難しい。

【0566】

前述した本実施形態のEMDシステムは、上述したような従来の問題を解決した。

すなわち、本実施形態のEMDシステムでは、コンテンツプロバイダがオーサリングしたデジタルコンテンツは、すべてコンテンツプロバイダ側で、コンテンツ形態や権利書データを作成し、コンテンツプロバイダ側のデータベースに管理しておく。コンテンツの権利書データに関しては、さらに第3の信頼機関であるEMDサービスセンタ（クリアリングハウス）で権威化し登録しておく。

こうすることで、コンテンツプロバイダの関係者が、デジタルコンテンツの権利処理ルールを完全に自分の管理下におくことができ、流通経路をコンテンツプロバイダ側で管理することを可能とする。また本件では、このコンテンツプロバイダ側で作成した権利書のデータの内容を、ユーザとの間に存在する流通業者が見ることができないような仕掛けを提供する。

また、本実施形態のEMDシステムでは、ROM型記録媒体を、ひとつの流通手段として考えて、そこに搭載するデジタルコンテンツの存在をROM型記録媒

体から遊離させる。流通手段、流通経路によらず、デジタルコンテンツ単体で、その存在価値を表現するコンテンツ形態を提案する。デジタルコンテンツはコンテンツプロバイダ側である規定の形式で管理されるので、ROM型記録媒体に、その形式のデジタルコンテンツを搭載すると考えることで、ROM型記録媒体で流通されようが、デジタルネットワークで流通されようが、ユーザホームネットワーク上では、ROM→RAM、ネットワーク→RAMにおいて共通の権利処理ルールを提供することが可能となる。デジタルコンテンツの販売セッションを、すべてコンテンツプロバイダが規定、管理する形式でおこなう。これにより、流通手段、流通経路によらない共通の権利処理が可能となる。また、このコンテンツプロバイダ側で規定されたコンテンツ形態は、デジタルコンテンツの売買をおこなう上での最小単位と定義することで、その後の流通過程で利用されるコンテンツ形態の種類に依存せず共通の権利処理ルールを提供することができる。ユーザホームネットワークで購入したときに生成される課金情報を、サービスプロバイダに返すのではなく、第3の信頼機関であるEMDサービスセンタに返し、そこからサービスプロバイダに返すことによりコンテンツの2次利用によるビジネスの問題点を解決した。

【0567】

【発明の効果】

以上説明したように、本発明によれば、データ提供装置が提供したコンテンツデータのデータ処理装置における取り扱いを、データ提供装置による権利書データに基づいて行わせることが可能になる。

その結果、データ提供装置の関係者によるコンテンツデータに係わる利益を適切に保護することが可能になると共に、当該関係者による監査の負担を軽減できる。

【図面の簡単な説明】

【図1】

図1は、本発明の第1実施形態のEMDシステムの全体構成図である。

【図2】

図2は、本発明のセキュアコンテナの概念を説明するための図である。

【図 3】

図 3 は、図 1 に示すコンテンツプロバイダの機能ブロック図であり、ユーザホームネットワークの SAM との間で送受信されるデータに関連するデータの流れを示す図である。

【図 4】

図 4 は、図 1 に示すコンテンツプロバイダの機能ブロック図であり、コンテンツプロバイダと EMD サービスセンタとの間で送受信されるデータに関連するデータの流れを示す図である。

【図 5】

図 5 は、図 1 に示すコンテンツプロバイダから SAM に送信されるセキュアコンテナのフォーマットを説明するための図である。

【図 6】

図 6 は、図 5 に示すコンテンツファイルに含まれるデータを詳細に説明するための図である。

【図 7】

図 7 は、図 5 に示すキーファイルに含まれるデータを詳細に説明するための図である。

【図 8】

図 8 は、コンテンツファイルに格納されるヘッダデータを説明するための図である。

【図 9】

図 9 は、コンテンツ ID を説明するための図である。

【図 1 0】

図 1 0 は、セキュアコンテナのディレクトリ構造を説明するための図である。

【図 1 1】

図 1 1 は、セキュアコンテナのハイパーリンク構造を説明するための図である。

【図 1 2】

図 1 2 は、本実施形態で用いられる ROM 型の記録媒体の第 1 の例を説明する

ための図である。

【図 1 3】

図 1 3 は、本実施形態で用いられる R O M 型の記録媒体の第 2 の例を説明するための図である。

【図 1 4】

図 1 4 は、本実施形態で用いられる R O M 型の記録媒体の第 3 の例を説明するための図である。

【図 1 5】

図 1 5 は、本実施形態で用いられる R A M 型の記録媒体の第 1 の例を説明するための図である。

【図 1 6】

図 1 6 は、本実施形態で用いられる R A M 型の記録媒体の第 2 の例を説明するための図である。

【図 1 7】

図 1 7 は、本実施形態で用いられる R A M 型の記録媒体の第 3 の例を説明するための図である。

【図 1 8】

図 1 8 は、コンテンツプロバイダから E M D サービスセンタに送信される登録要求用モジュールを説明するための図である。

【図 1 9】

図 1 9 は、コンテンツプロバイダから E M D サービスセンタへの登録処理の手順を示すフローチャートである。

【図 2 0】

図 2 0 は、コンテンツプロバイダにおける説明の作成処理の手順を示すフローチャートである。

【図 2 1】

図 2 1 は、コンテンツプロバイダにおける説明の作成処理の手順を示すフローチャートである。

【図 2 2】

図 2 2 は、コンテンツプロバイダにおける説明の作成処理の手順を示すフローチャートである。

【図 2 3】

図 2 3 は、図 1 に示す EMD サービスセンタの機能ブロック図であり、コンテンツプロバイダとの間で送受信されるデータに関連するデータの流れを示す図である。

【図 2 4】

図 2 4 は、図 1 に示す EMD サービスセンタの機能ブロック図であり、SAM および図 1 に示す決済機関との間で送受信されるデータに関連するデータの流れを示す図である。

【図 2 5】

図 2 5 は、図 1 に示すユーザホームネットワーク内のネットワーク機器の構成図である。

【図 2 6】

図 2 6 は、図 1 に示すユーザホームネットワーク内の SAM の機能ブロック図であり、コンテンツプロバイダから受信したセキュアコンテンツを復号するまでのデータの流れを示す図である。

【図 2 7】

図 2 7 は、図 2 5 に示す外部メモリに記憶されるデータを説明するための図である。

【図 2 8】

図 2 8 は、スタックメモリに記憶されるデータを説明するための図である。

【図 2 9】

図 2 9 は、図 1 に示すユーザホームネットワーク内のネットワーク機器のその他の構成図である。

【図 3 0】

図 3 0 は、図 2 6 に示す記憶部に記憶されるデータを説明するための図である。

【図 3 1】

図 3 1 は、図 1 に示すユーザホームネットワーク内の SAM の機能ブロック図であり、コンテンツデータを利用・購入する処理などに関連するデータの流れを示す図である。

【図 3 2】

図 3 2 は、図 2 5 に示すネットワーク機器のダウンロードメモリにダウンロードされた既に購入形態が決定されたコンテンツファイルを、AV 機器の SAM に転送する場合の転送元の SAM 内での処理の流れを説明するための図である。

【図 3 3】

図 3 3 は、図 3 2 に示す場合における転送元の SAM 内でのデータの流れを示す図である。

【図 3 4】

図 3 4 は、購入形態が決定したセキュアコンテナのフォーマットを説明するための図である。

【図 3 5】

図 3 5 は、図 3 2 に示す場合において、転送先の SAM において、入力したコンテンツファイルなどを、RAM 型あるいは ROM 型の記録媒体（メディア）に書き込む際のデータの流れを示す図である。

【図 3 6】

図 3 6、コンテンツの購入形態が未決定の図 7 に示す ROM 型の記録媒体をユーザホームネットワークがオフラインで配給を受けた場合に、AV 機器において購入形態を決定する際の処理の流れを説明するための図である。

【図 3 7】

図 3 7 は、図 3 6 に示す場合において、SAM 内でのデータの流れを示す図である。

【図 3 8】

図 3 8 は、ユーザホームネットワーク内の AV 機器において購入形態が未決定の ROM 型の記録媒体からセキュアコンテナを読み出して、これを他の AV 機器に転送して RAM 型の記録媒体に書き込む際の処理の流れを説明するための図である。

【図 39】

図 39 は、図 38 に示す場合における転送元の SAM 内でのデータの流れを示す図である。

【図 40】

図 40 は、図 38 において、転送元の SAM から転送先の SAM に転送されるセキュアコンテンツのフォーマットを説明するための図である。

【図 41】

図 41 は、図 38 に示す場合における転送先の SAM 内でのデータの流れを示す図である。

【図 42】

図 42 は、図 1 に示すコンテンツプロバイダ、EMD サービスセンタおよび SAM の相互間で、イン・バンド方式およびアウト・オブ・バンド方式で、送受信されるデータのフォーマットを説明するための図である。

【図 43】

図 43 は、図 1 に示すコンテンツプロバイダ、EMD サービスセンタおよび SAM の相互間で、イン・バンド方式およびアウト・オブ・バンド方式で、送受信されるデータのフォーマットを説明するための図である。

【図 44】

図 44 は、ユーザホームネットワーク内でのバスへの機器の接続形態の一例を説明するための図である。

【図 45】

図 45 は、SAM が作成する SAM 登録リストのデータフォーマットを説明するための図である。

【図 46】

図 46 は、EMD サービスセンタが作成する SAM 登録リストのデータフォーマットを説明するための図である。

【図 47】

図 47 は、図 1 に示すコンテンツプロバイダの全体動作のフローチャートである。

【図 4 8】

図 4 8 は、第 1 実施形態の EMD システムにおいて用いられるセキュアコンテナの配送プロトコルの一例を説明するための図である。

【図 4 9】

図 4 9 は、本発明の第 1 実施形態の第 2 変形例を説明するための図である。

【図 5 0】

図 5 0 は、本発明の第 1 実施形態の第 3 変形例を説明するための図である。

【図 5 1】

図 5 1 は、本発明の第 1 実施形態の第 4 変形例において第 1 の手法を採用した場合を説明するための図である。

【図 5 2】

図 5 2 は、本発明の第 1 実施形態の第 4 変形例において第 2 の手法を採用した場合を説明するための図である。

【図 5 3】

図 5 3 は、本発明の第 1 実施形態の第 5 変形例を説明するための図である。

【図 5 4】

図 5 4 は、本発明の第 1 実施形態の第 6 変形例の第 1 のパターンを説明するための図である。

【図 5 5】

図 5 5 は、本発明の第 1 実施形態の第 6 変形例の第 2 のパターンを説明するための図である。

【図 5 6】

図 5 6 は、本発明の第 1 実施形態の第 6 変形例の第 3 のパターンを説明するための図である。

【図 5 7】

図 5 7 は、本発明の第 1 実施形態の第 6 変形例の第 4 のパターンを説明するための図である。

【図 5 8】

図 5 8 は、本発明の第 1 実施形態の第 6 変形例の第 5 のパターンを説明するた

めの図である。

【図 59】

図 59 は、本発明の第 2 実施形態の EMD システムの全体構成図である。

【図 60】

図 60 は、図 59 に示すコンテンツプロバイダの機能ブロック図であり、サービスプロバイダに送信されるセキュアコンテンツに関するデータの流れを示す図である。

【図 61】

図 61 は、コンテンツプロバイダにおいて行われるセキュアコンテンツの配送処理の手順を示すフローチャートである。

【図 62】

図 62 は、コンテンツプロバイダにおいて行われるセキュアコンテンツの配送処理の手順を示すフローチャートである。

【図 63】

図 63 は、図 59 に示すサービスプロバイダの機能ブロック図であり、ユーザホームネットワークとの間で送受信されるデータの流れを示す図である。

【図 64】

図 64 は、サービスプロバイダにおいて行われるセキュアコンテンツの作成処理の手順を示すフローチャートである。

【図 65】

図 65 は、図 59 に示すサービスプロバイダからユーザホームネットワークに送信されるセキュアコンテンツのフォーマットを説明するための図である。

【図 66】

図 66 は、図 65 に示すセキュアコンテンツに格納されたコンテンツファイルの送信形態を説明するための図である。

【図 67】

図 67 は、図 65 に示すセキュアコンテンツに格納されたキーファイルの送信形態を説明するための図である。

【図 68】

図 68 は、図 59 に示すサービスプロバイダの機能ブロック図であり、EMD サービスセンタとの間で送受信されるデータの流れを示す図である。

【図 69】

図 69 は、サービスプロバイダから EMD サービスセンタに送信されるプライスタグ登録要求用モジュールのフォーマットを説明するための図である。

【図 70】

図 70 は、図 59 に示す EMD サービスセンタの機能ブロック図であり、サービスプロバイダとの間で送受信されるデータに関連するデータの流れを示す図である。

【図 71】

図 71 は、図 59 に示す EMD サービスセンタの機能ブロック図であり、コンテンツプロバイダとの間で送受信されるデータに関連するデータの流れを示す図である。

【図 72】

図 72 は、図 59 に示す EMD サービスセンタの機能ブロック図であり、SAM との間に送受信されるデータに関連するデータの流れを示す図である。

【図 73】

図 73 は、利用履歴データの内容を説明するための図である。

【図 74】

図 74 は、図 59 に示すネットワーク機器の構成図である。

【図 75】

図 75 は、図 74 に示す CA モジュールの機能ブロック図である。

【図 76】

図 76 は、図 74 に示す SAM の機能ブロック図であり、セキュアコンテナを入力してから復号するまでのデータの流れを示す図である。

【図 77】

図 77 は、図 76 に示す記憶部に記憶されるデータを説明するための図である。

【図 78】

図 78 は、図 74 に示す SAM の機能ブロック図であり、コンテンツの購入・利用形態を決定する場合などのデータの流れを示す図である。

【図 79】

図 79 は、SAM におけるセキュアコンテナの購入形態の決定処理の手順を示すフローチャートである。

【図 80】

図 80 は、購入形態が決定された後のキーファイルのフォーマットを説明するための図である。

【図 81】

図 81 は、図 74 に示すネットワーク機器のダウンロードメモリにダウンロードされた既に購入形態が決定されたコンテンツファイルを、AV 機器の SAM に転送する場合の転送先の SAM 内での処理の流れを説明するための図である。

【図 82】

図 82 は、図 81 に示す場合の転送元の SAM 内でのデータの流れを示す図である。

【図 83】

図 83 は、図 81 に示す場合の転送先の SAM 内でのデータの流れを示す図である。

【図 84】

図 84 は、図 59 に示す EMD システムの全体動作のフローチャートである。

【図 85】

図 85 は、図 59 に示す EMD システムの全体動作のフローチャートである。

【図 86】

図 86 は、第 2 実施形態の EMD システムにおけるサービスプロバイダからユーザホームネットワークへのセキュアコンテナの配送形態の一例を説明するための図である。

【図 87】

図 87 は、第 2 実施形態の EMD システムが採用するセキュアコンテナの配送プロトコルの一例を説明するための図である。

【図 8 8】

図 8 8 は、図 8 7 においてユーザホームネットワークからサービスプロバイダ 310 へのセキュアコンテナなどを配送する際に用いられる配送プロトコルを説明するための図である。

【図 8 9】

図 8 9 は、図 8 7 においてコンテンツプロバイダから EMD サービスセンタへのキーファイルなどを配送する際に用いられる配送プロトコルを説明するための図である。

【図 9 0】

図 9 0 は、図 8 7 においてサービスプロバイダから EMD サービスセンタへのプライスタグデータ 312などを配送する際に用いられる配送プロトコルを説明するための図である。

【図 9 1】

図 9 1 は、図 8 7 においてユーザホームネットワーク内でセキュアコンテナなどを配送する際に用いられる配送プロトコルを説明するための図である。

【図 9 2】

図 9 2 は、デジタル放送のデータ放送方式に XML / SMIL / BML を利用した場合のプロトコル層へのセキュアコンテナのインプリメント形態を説明するための図である。

【図 9 3】

図 9 3 は、デジタル放送のデータ放送方式に MHEG を利用した場合のプロトコル層へのセキュアコンテナのインプリメント形態を説明するための図である。

【図 9 4】

図 9 4 は、インターフェイスのデータ放送方式に XML / SMIL を利用した場合のプロトコル層へのセキュアコンテナのインプリメント形態を説明するための図である。

【図 9 5】

図 9 5 は、ユーザホームネットワークから EMD サービスセンタに利用履歴データなどを配送する際に用いられる配送プロトコルを説明するための図である。

【図 9 6】

図 9 6 は、ユーザホームネットワーク内においてセキュアコンテナなどを配送する際に用いられる配送プロトコルを説明するための図である。

【図 9 7】

図 9 7 は、本発明の第 2 実施形態の第 1 変形例に係わる 2 個のサービスプロバイダを用いた EMD システムの構成図である。

【図 9 8】

図 9 8 は、本発明の第 2 実施形態の第 2 変形例に係わる複数のコンテンツプロバイダを用いた EMD システムの構成図である。

【図 9 9】

図 9 9 は、本発明の第 2 実施形態の第 3 変形例に係わる EMD システムの構成図である。

【図 1 0 0】

図 1 0 0 は、本発明の第 2 実施形態の第 4 変形例に係わる EMD システムの構成図である。

【図 1 0 1】

図 1 0 1 は、公開鍵証明書データの取得ルートの形態を説明するための図である。

【図 1 0 2】

図 1 0 2 は、コンテンツプロバイダの公開鍵証明書データを無効にする場合の処理を説明するための図である。

【図 1 0 3】

図 1 0 3 は、サービスプロバイダの公開鍵証明書データを無効にする場合の処理を説明するための図である。

【図 1 0 4】

図 1 0 4 は、SAM の公開鍵証明書データを無効にする場合の処理を説明するための図である。

【図 1 0 5】

図 1 0 5 は、SAM の公開鍵証明書データを無効にする場合のその他の処理を

説明するための図である。

【図 106】

図 106 は、図 47 に示す EMD システムにおいて、EMD サービスセンタの代わりに権利管理用クリアリングハウスおよび電子決済用クリアリングハウスを設けた場合を説明するための図である。

【図 107】

図 107 は、図 106 に示す権利管理用クリアリングハウスおよび電子決済用クリアリングハウスを単体の EMD サービスセンタ内に設けた場合の EMD システムの構成図である。

【図 108】

図 108 は、サービスプロバイダが電子決済用クリアリングハウスに直接的に決済を行う場合の EMD システムの構成図である。

【図 109】

図 109 は、コンテンツプロバイダが電子決済用クリアリングハウスに直接的に決済を行う場合の EMD システムの構成図である。

【図 110】

図 110 は、コンテンツプロバイダが権利管理用クリアリングハウスおよび電子決済用クリアリングハウスの双方の機能をさらに備えている場合の EMD システムの構成図である。

【図 111】

図 111 は、本発明の第 2 実施形態の第 8 変形例において、図 47 に示すコンテンツプロバイダからサービスプロバイダに提供されるセキュアコンテナのフォーマットを説明するための図である。

【図 112】

図 112 は、図 111 に示すコンテンツファイルとキーファイルとの間のディレクトリ構造データによるリンク関係を説明するための図である。

【図 113】

図 113 は、コンテンツファイルとキーファイルとの間のディレクトリ構造のその他の例を説明するための図である。

【図 114】

図 114 は、本発明の第 2 実施形態の第 8 変形例において、図 47 に示すサービスプロバイダから SAM に提供されるセキュアコンテナのフォーマットを説明するための図である。

【図 115】

図 115 は、コンポジット型のセキュアコンテナのデータフォーマットの第 1 の概念を説明するための図である。

【図 116】

図 116 は、コンポジット型のセキュアコンテナのデータフォーマットの第 2 の概念を説明するための図である。

【図 117】

図 117 は、本発明の第 2 実施形態の第 8 変形例に係わる EMD システムにおいて第 1 の手法を採用した場合を説明するための図である。

【図 118】

図 118 は、本発明の第 2 実施形態の第 8 変形例に係わる EMD システムにおいて第 2 の手法を採用した場合を説明するための図である。

【図 119】

図 119 は、本発明の第 2 実施形態の第 8 変形例に係わる EMD システムにおいてファイル形式を採用しない場合のデータフォーマットを説明するための図である。

【図 120】

図 120 は、本発明の第 2 実施形態の第 10 変形例に係わる EMD システムの構成図である。

【図 121】

図 121 は、本発明の第 2 実施形態の第 11 変形例の第 1 のパターンに係わる EMD システムの構成図である。

【図 122】

図 122 は、本発明の第 2 実施形態の第 11 変形例の第 2 のパターンに係わる EMD システムの構成図である。

【図 1 2 3】

図 1 2 3 は、本発明の第 2 実施形態の第 1 1 変形例の第 3 のパターンに係わる EMD システムの構成図である。

【図 1 2 4】

図 1 2 4 は、本発明の第 2 実施形態の第 1 1 変形例の第 4 のパターンに係わる EMD システムの構成図である。

【図 1 2 5】

図 1 2 5 は、本発明の第 2 実施形態の第 1 1 変形例の第 5 のパターンに係わる EMD システムの構成図である。

【図 1 2 6】

図 1 2 6 は、本発明の第 2 実施形態の第 9 変形例に係わる EMD システムの構成図である。

【図 1 2 7】

図 1 2 7 は、本発明の第 2 実施形態におけるセキュアコンテナのファイル包括大小関係を説明するための図である。

【図 1 2 8】

図 1 2 8 は、本発明の第 3 実施形態の EMD システムを説明するための図である。

【図 1 2 9】

図 1 2 9 は、図 1 2 8 に示す EMD サービスセンタの機能ブロック図である。

【図 1 3 0】

図 1 3 0 は、本発明の第 3 実施形態の EMD システムの変形例を説明するための図である。

【図 1 3 1】

図 1 3 1 は本発明の第 4 実施形態の EMD システムを説明するための図である。

【図 1 3 2】

図 1 3 2 は本発明の第 4 実施形態の EMD システムの変形例を説明するための図である。

【図 1 3 3】

図 1 3 3 は本発明の第 5 実施形態の EMD システムを説明するための図である。

【図 1 3 4】

図 1 3 4 は本発明の第 5 実施形態の EMD システムの変形例を説明するための図である。

【図 1 3 5】

図 1 3 5 は本発明の第 5 実施形態の EMD システムのその他の変形例を説明するための図である。

【図 1 3 6】

図 1 3 6 は本発明の第 6 実施形態の EMD システムを説明するための図である。

【図 1 3 7】

図 1 3 7 は本発明の第 6 実施形態の EMD システムの変形例を説明するための図である。

【図 1 3 8】

図 1 3 8 は本発明の第 6 実施形態の EMD システムのその他の変形例を説明するための図である。

【図 1 3 9】

図 1 3 9 は本発明の第 7 実施形態の EMD システムを説明するための図である。

【図 1 4 0】

図 1 4 0 は本発明の第 7 実施形態の EMD システムの変形例を説明するための図である。

【図 1 4 1】

図 1 4 1 は本発明の第 7 実施形態の EMD システムのその他の変形例を説明するための図である。

【図 1 4 2】

図 1 4 2 は本発明の第 8 実施形態の EMD システムを説明するための図である

【図 143】

図 143 は本発明の第 9 実施形態の EMD システムを説明するための図である

【図 144】

図 144 は、コンテンツプロバイダにおいてキーファイルを作成した場合のキーファイルのフォーマットを説明するための図である。

【図 145】

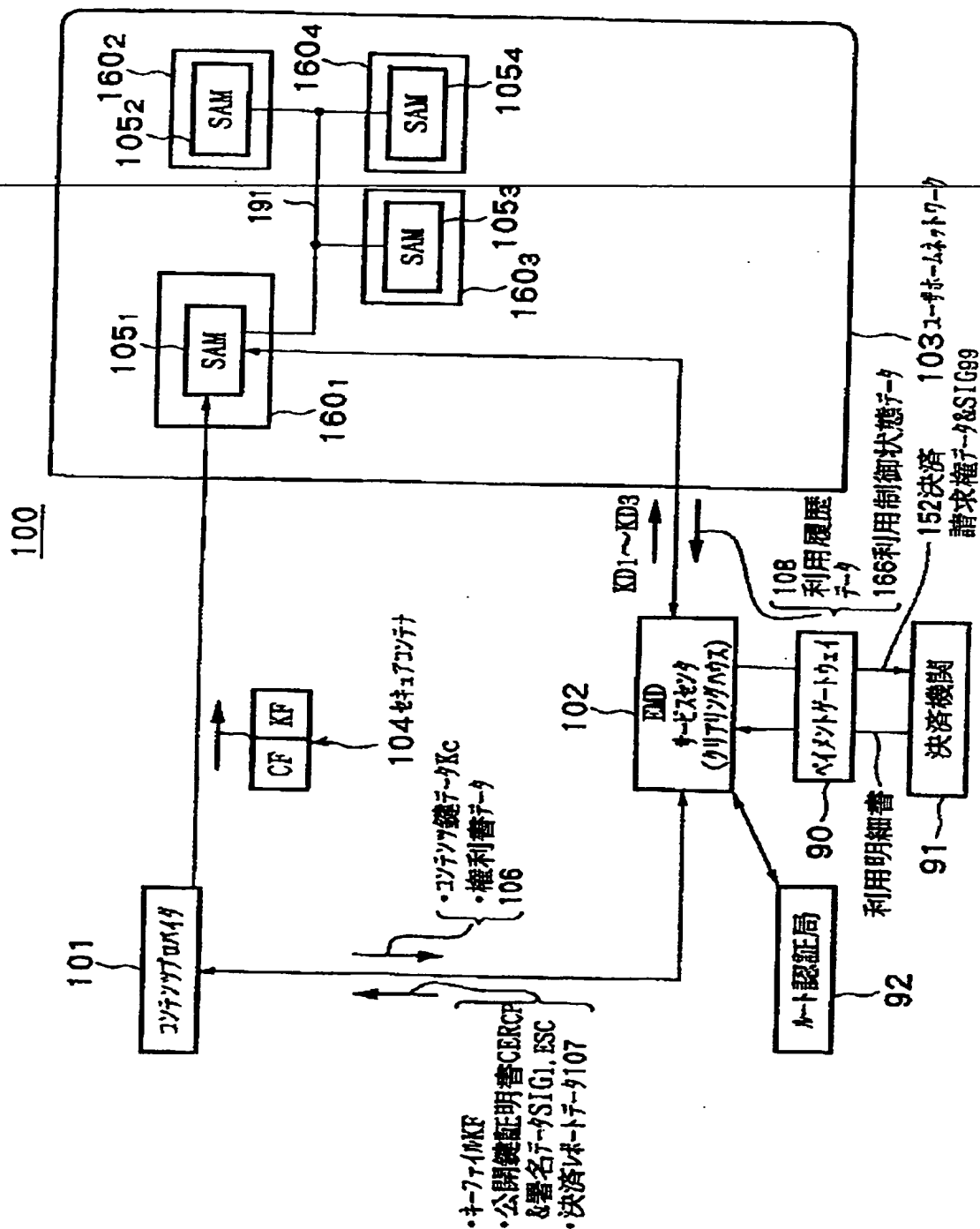
図 145 は、従来の EMD システムの構成図である。

【符号の説明】

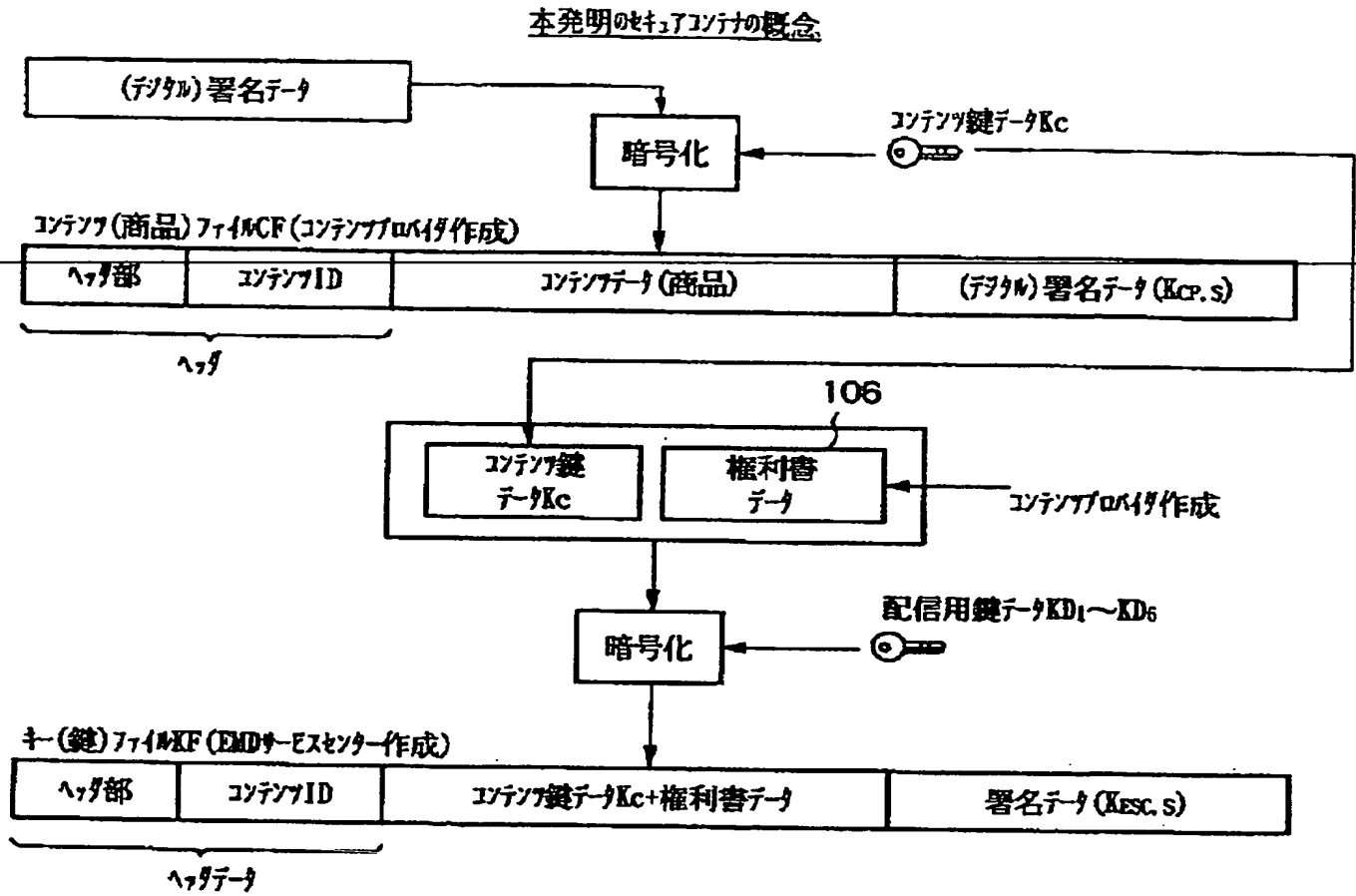
90…ペイメントゲートウェイ、91…決済機関、92…ルート認証局、100, 300…EMD システム、101, 301…コンテンツプロバイダ、102, 302…EMD サービスセンタ、103, 303…ユーザホームネットワーク、104, 304…セキュアコンテナ、105₁～105₄, 305₁～305₄…SAM、106…権利書データ、107, 307…決済レポートデータ、108, 308…利用履歴データ、160₁…ネットワーク機器、160₂～160₄…AV 機器、152, 152c, 152s…決済請求権データ、191…バス、310…サービスプロバイダ、311…CA モジュール、312…プライスタグデータ、CF…コンテンツファイル、KF…キーファイル、Kc…コンテンツ鍵データ

【書類名】 図面

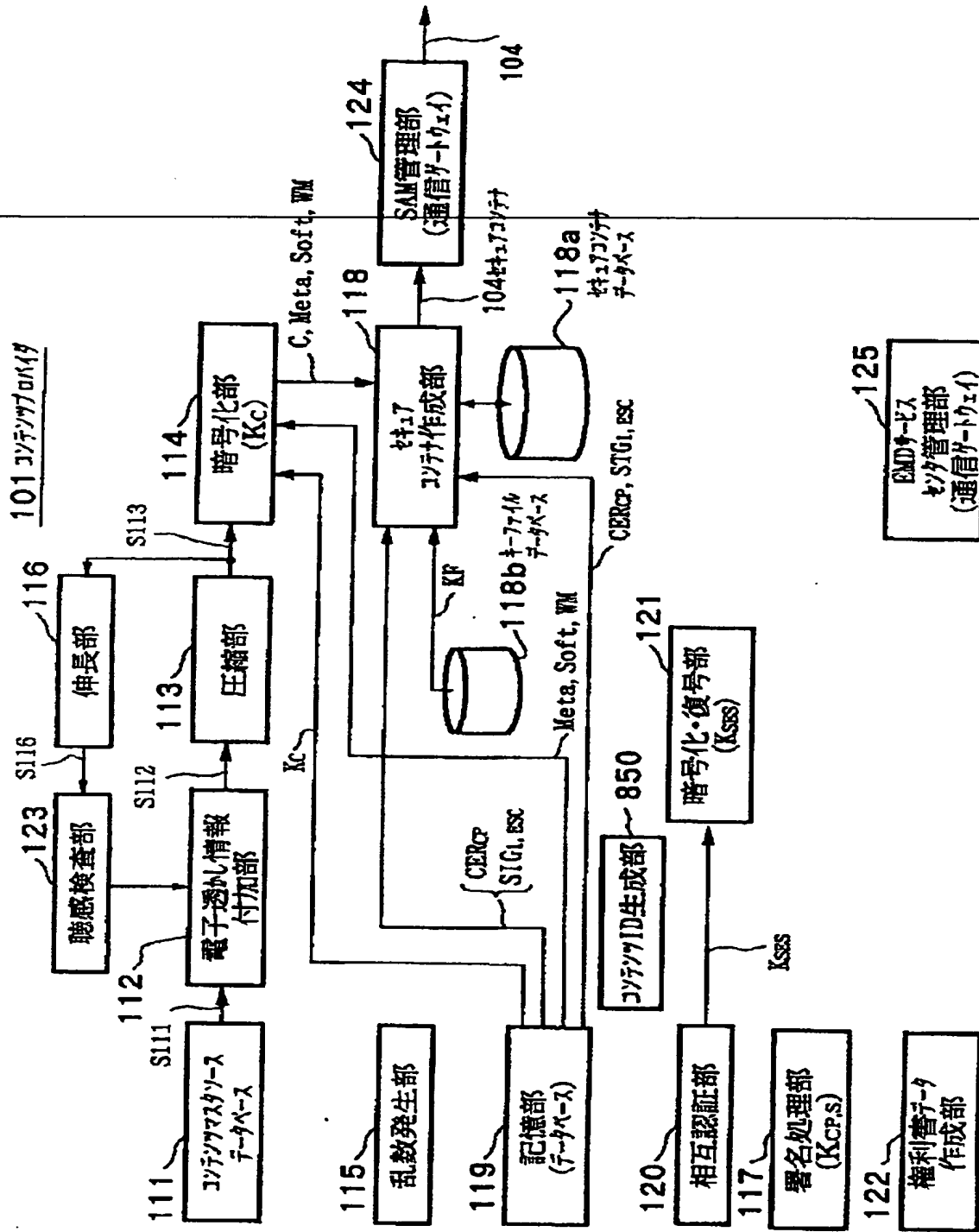
【図 1】



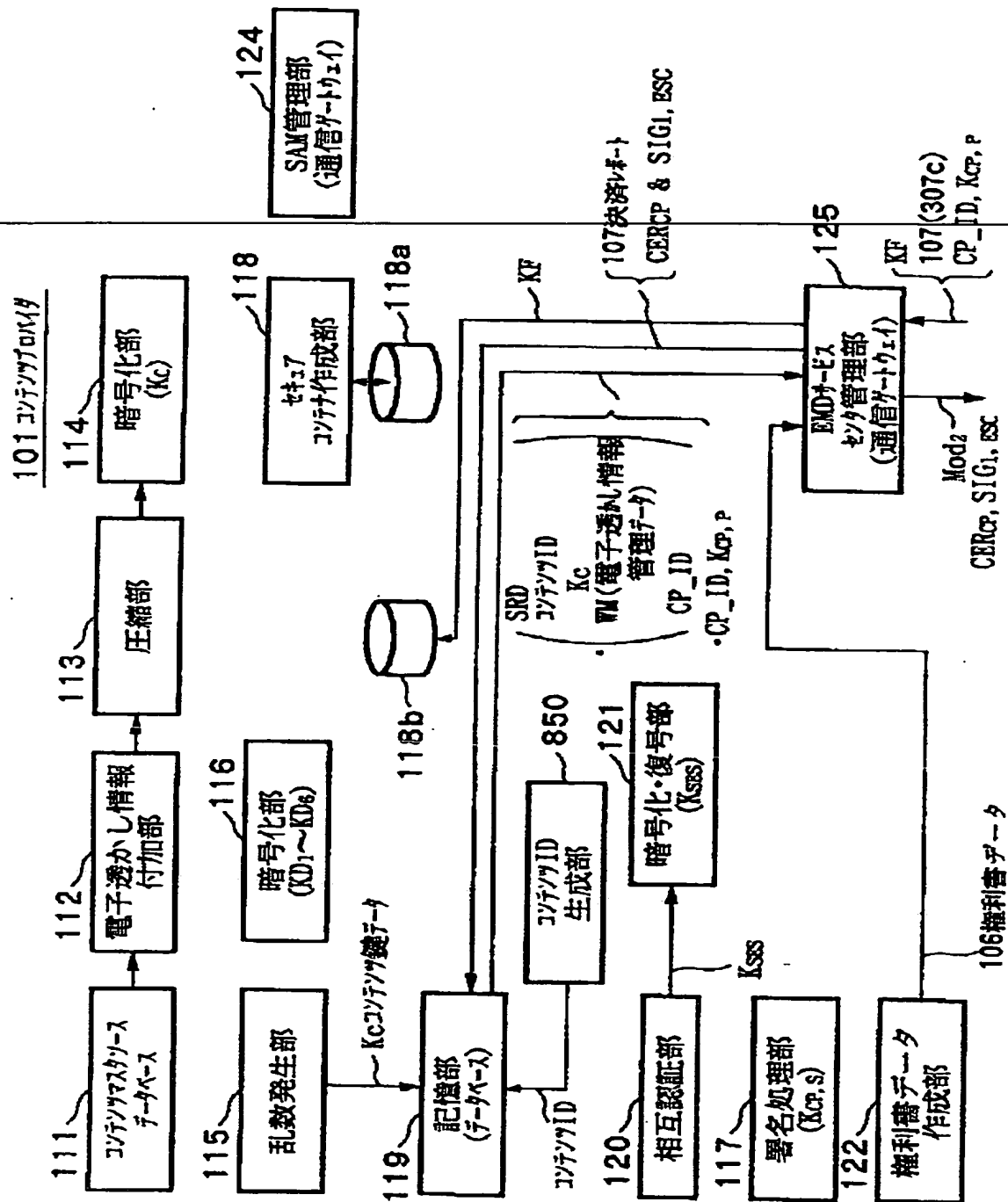
【図 2】



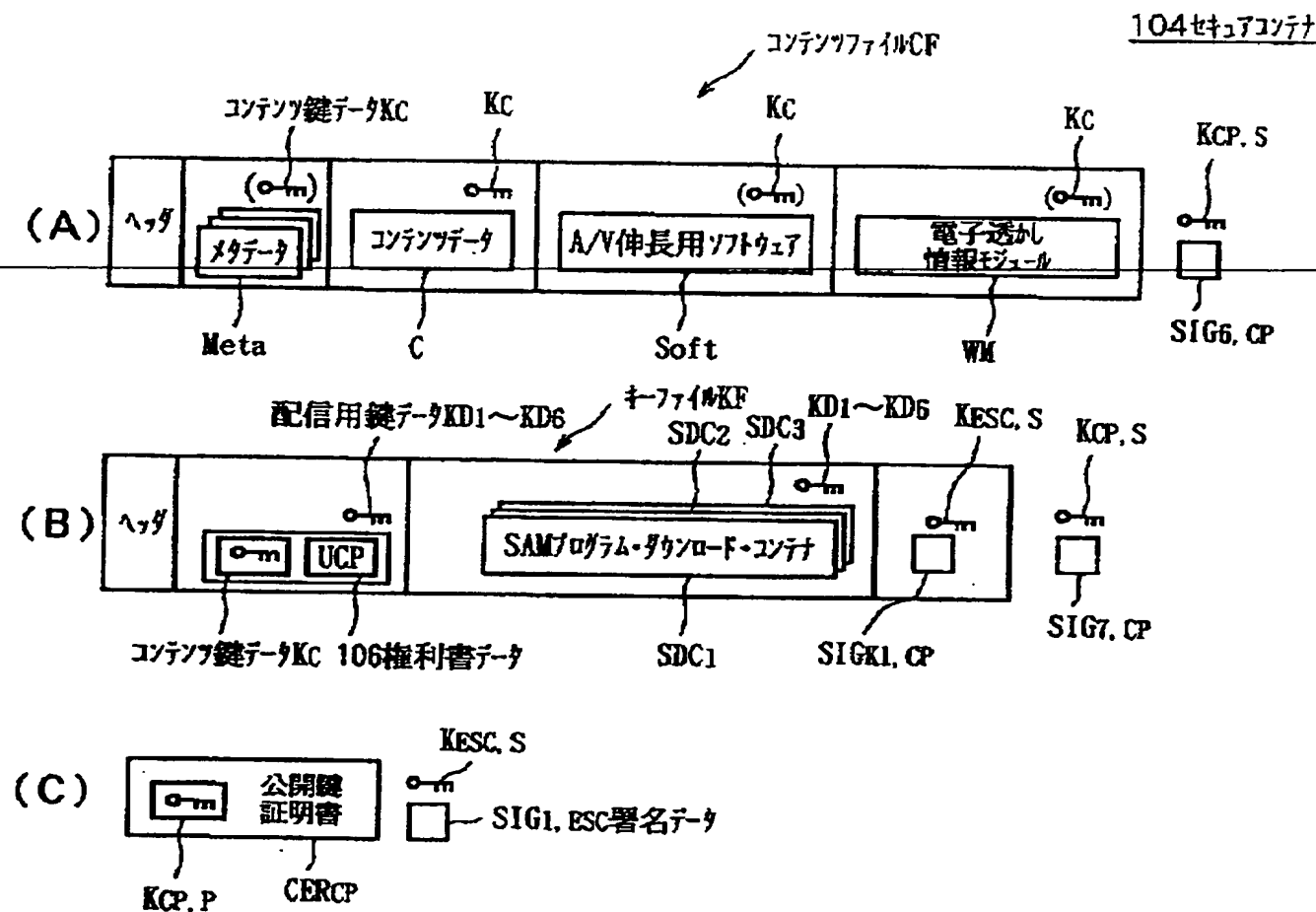
【図 3】



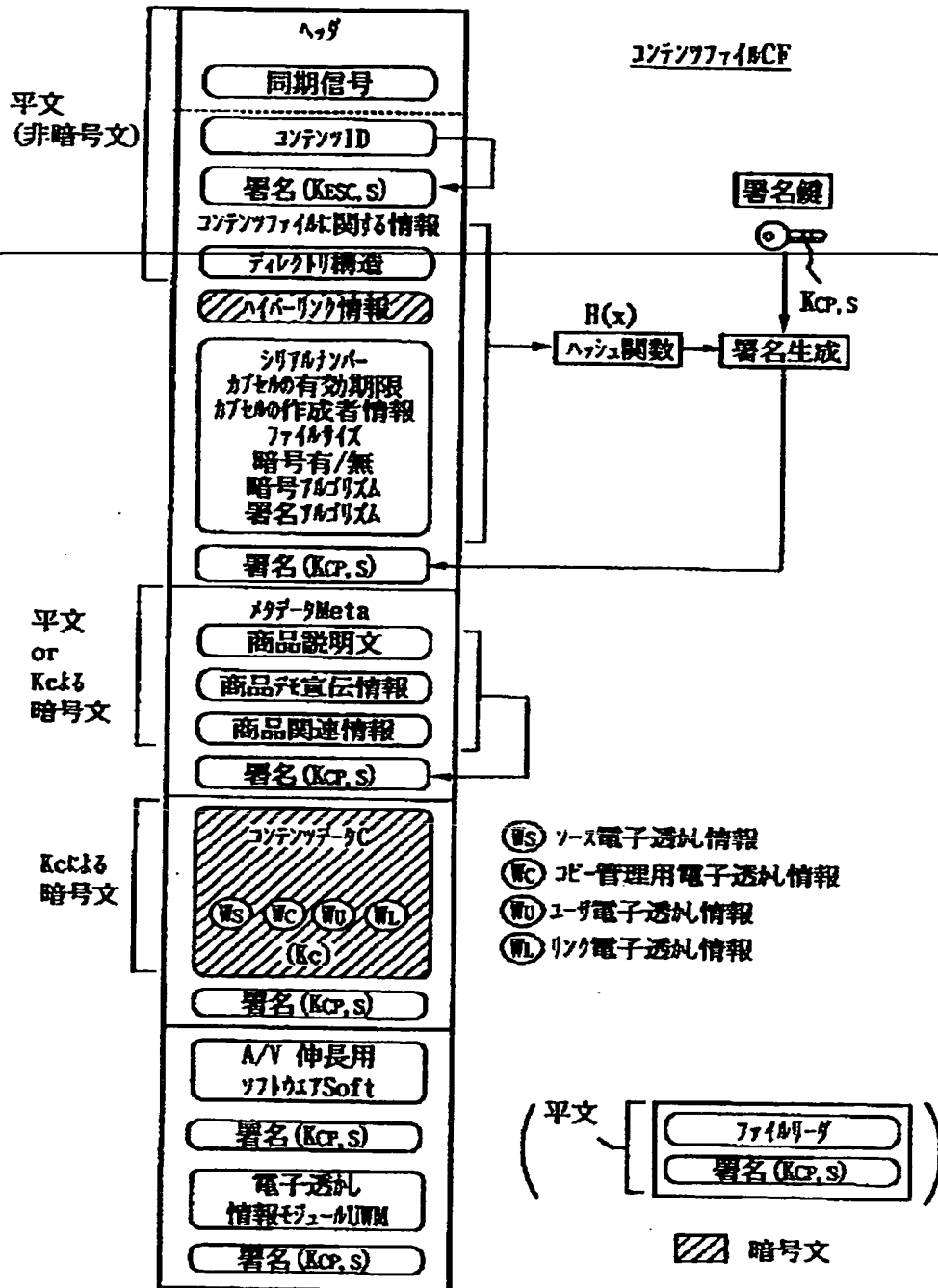
【図4】



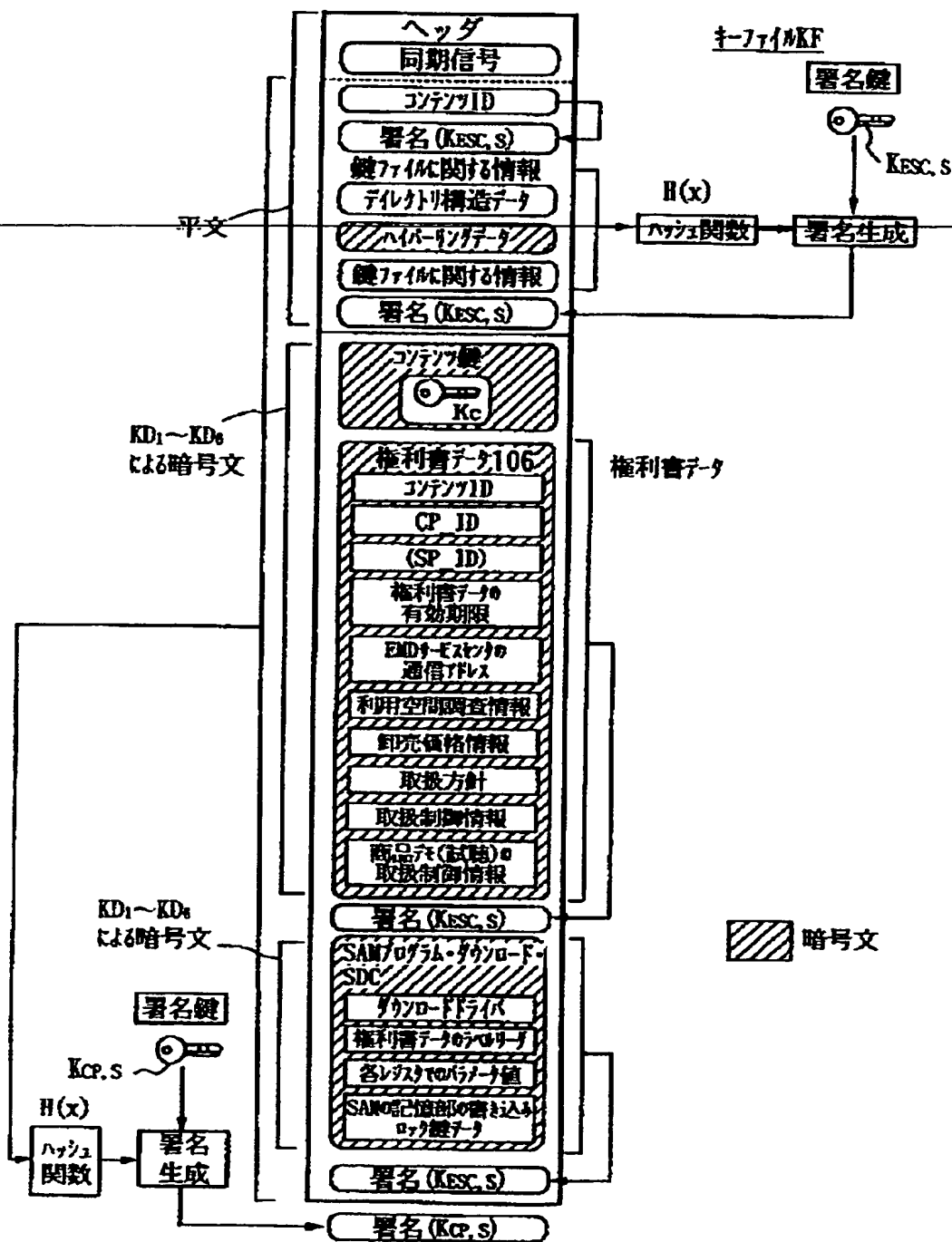
【図 5】



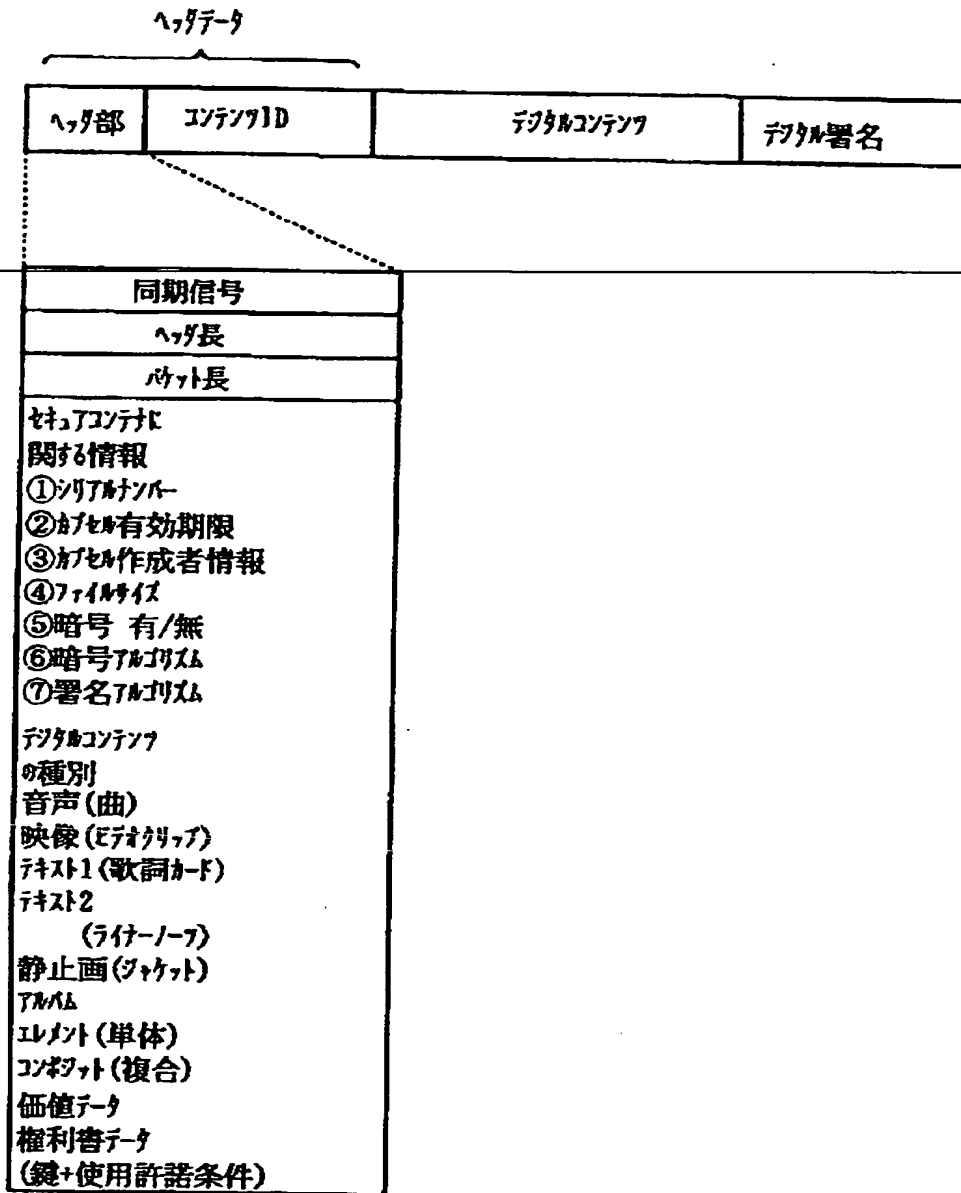
【図6】



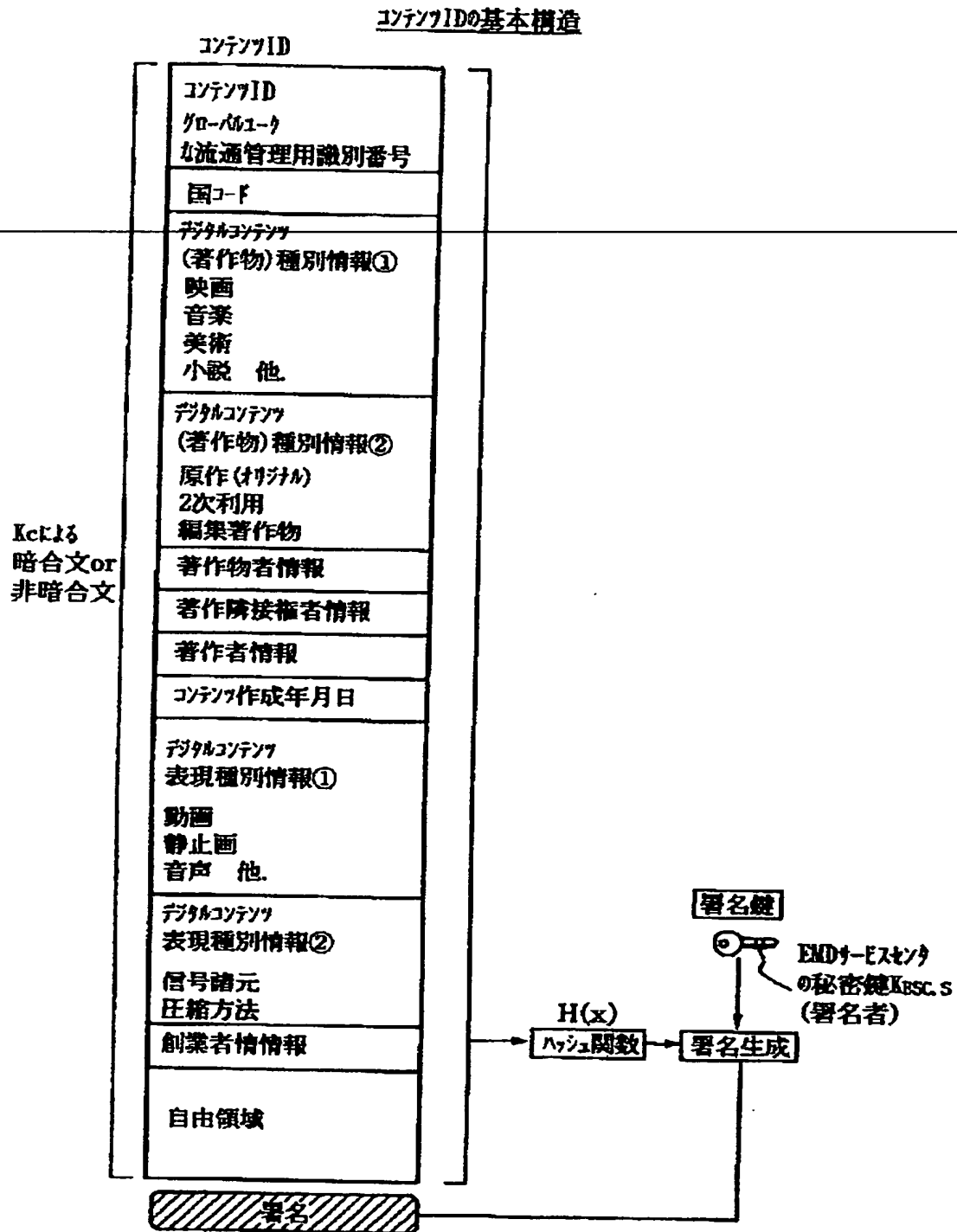
【図 7】



【図 8】

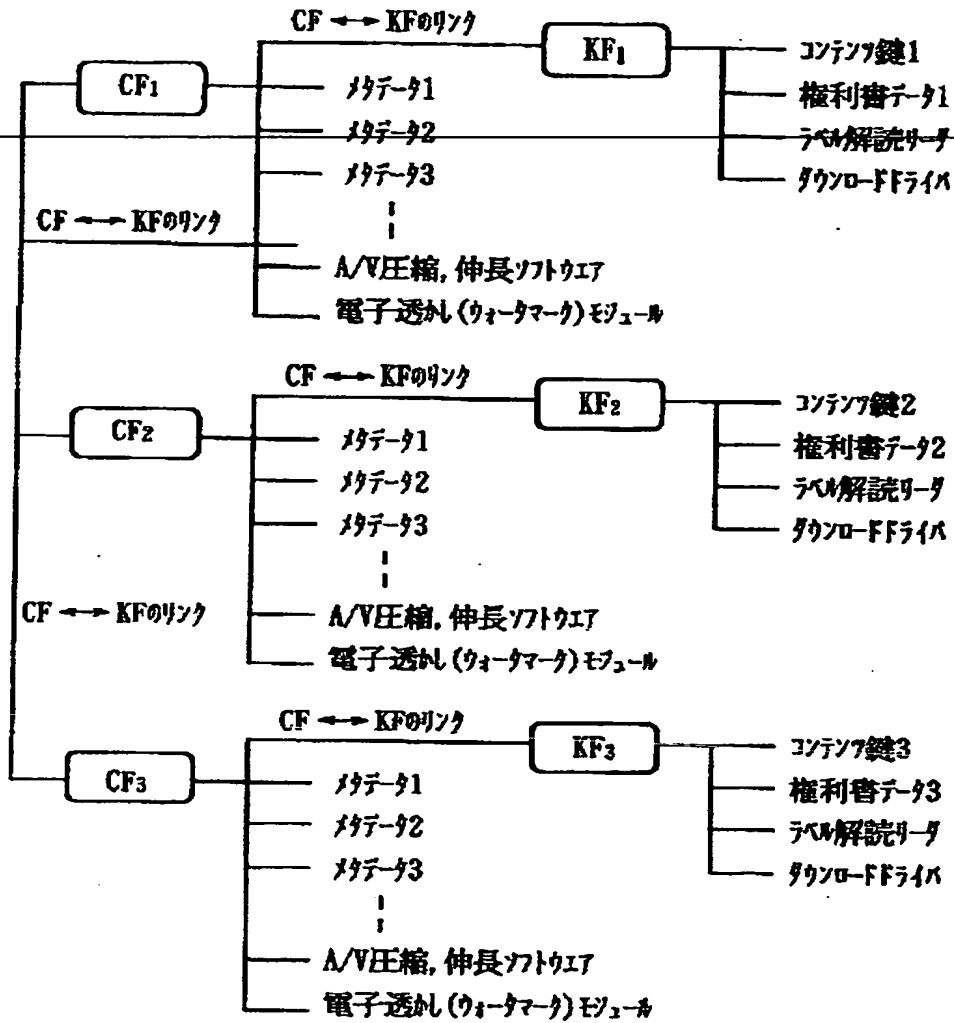


【図 9】

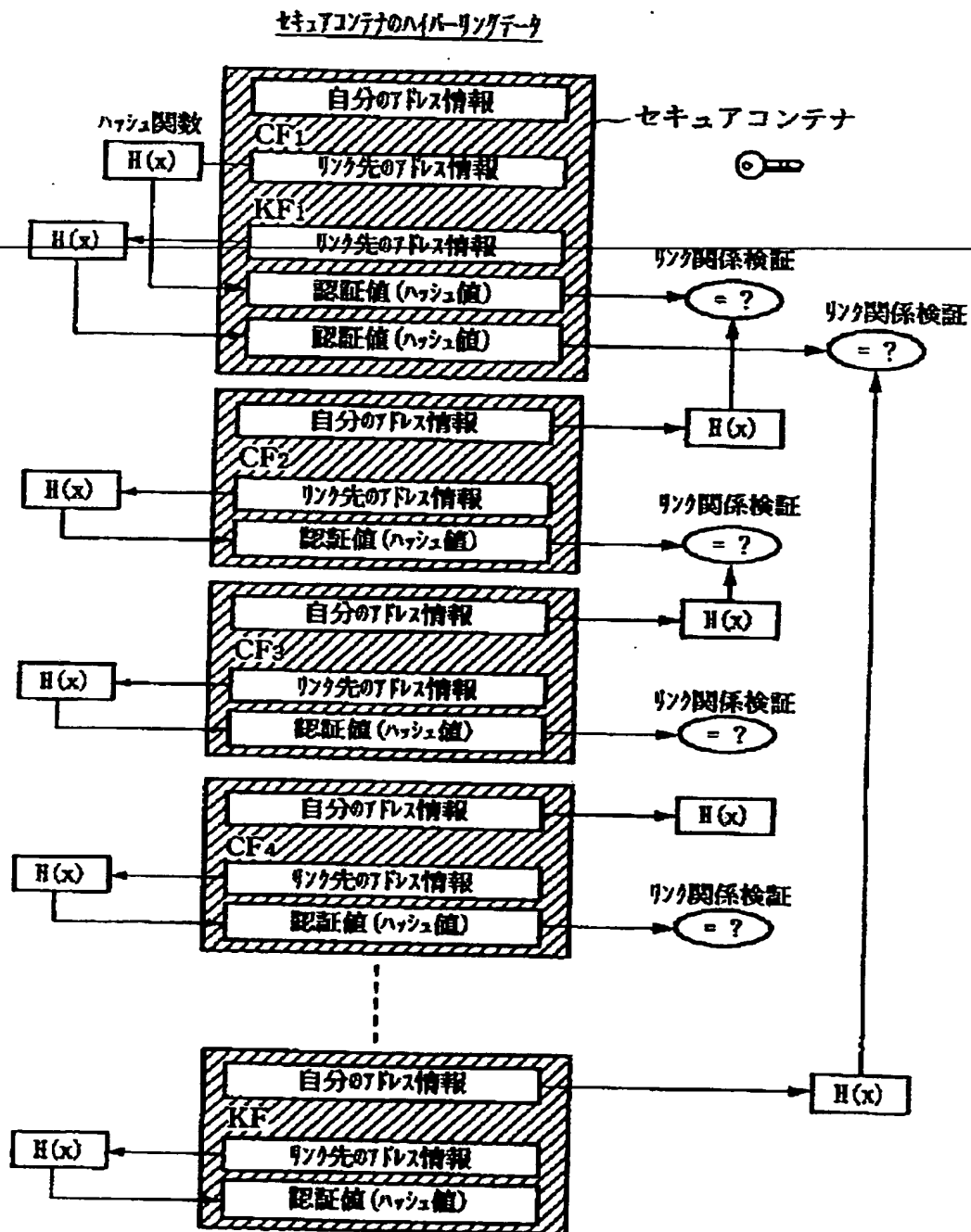


【図 1 0】

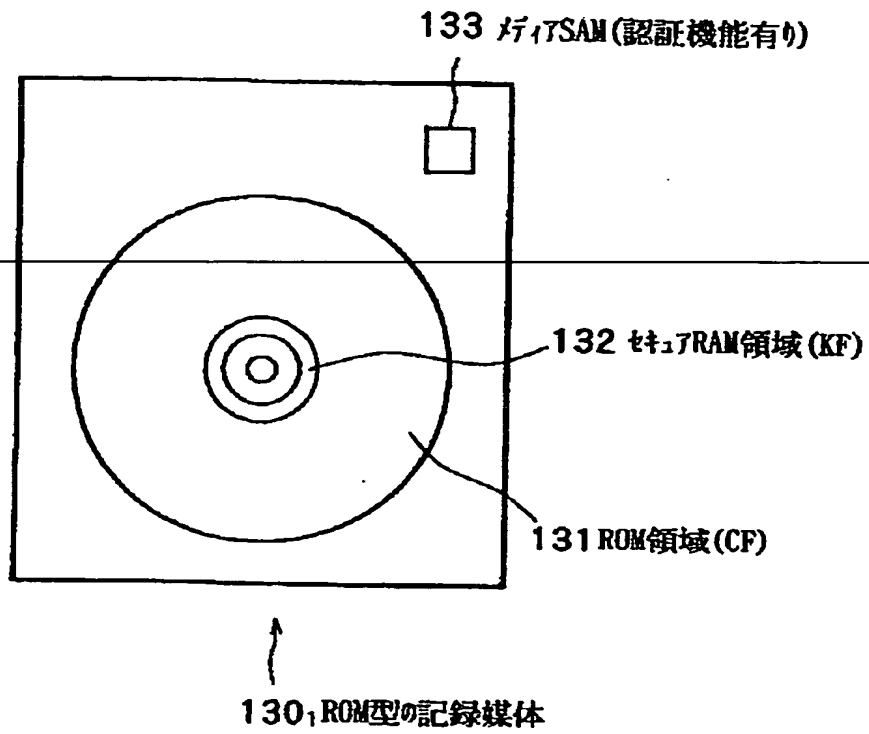
セミアコンテナのディレトリ構造



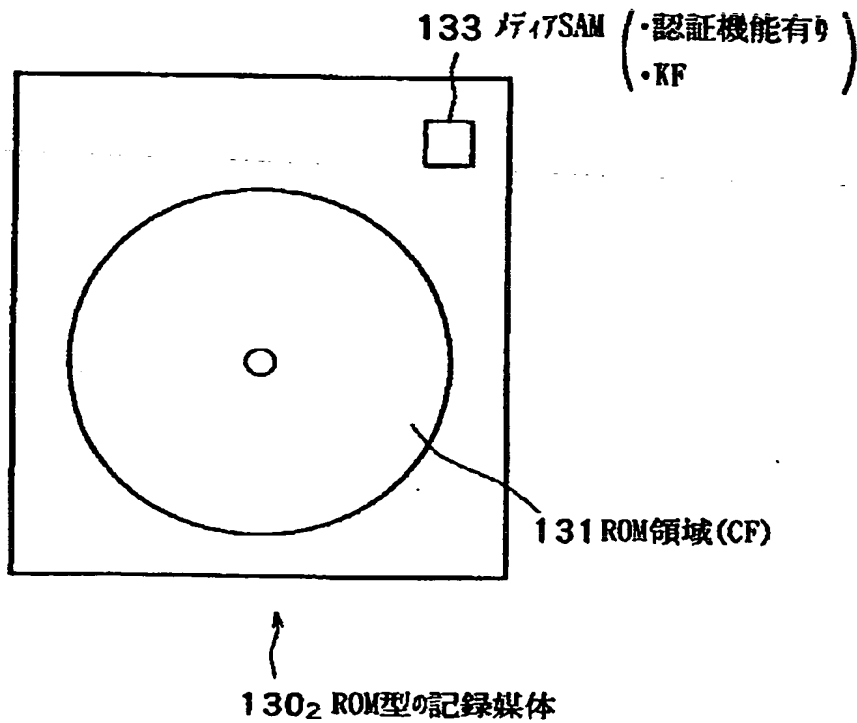
【図 11】



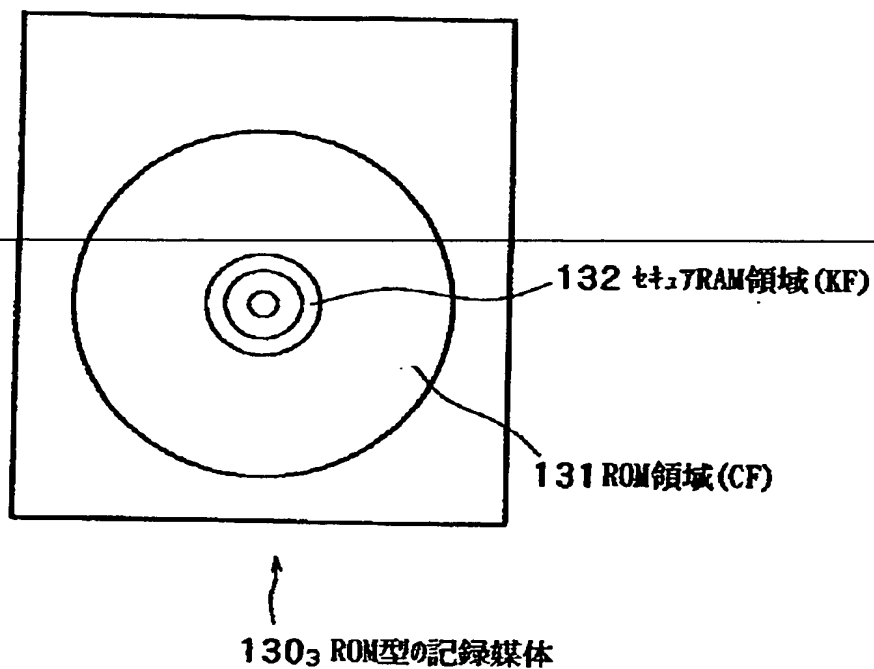
【図 1 2】



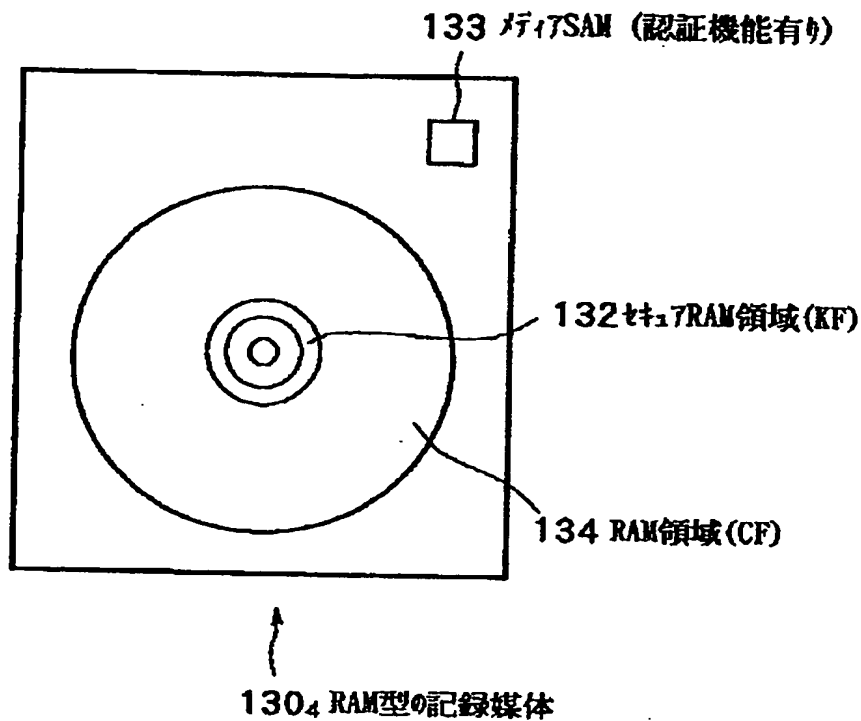
【図 1 3】



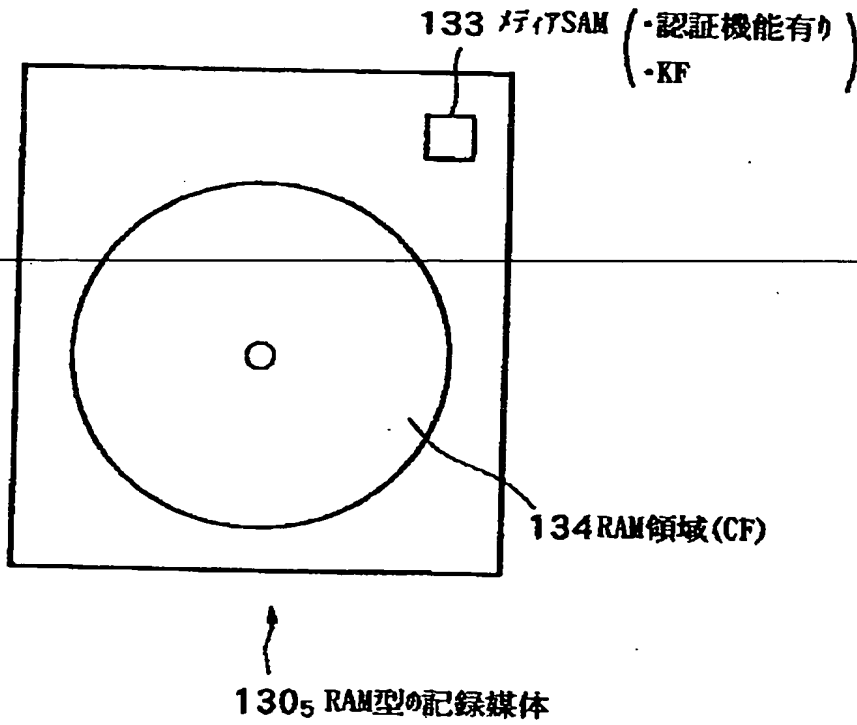
【図 1 4】



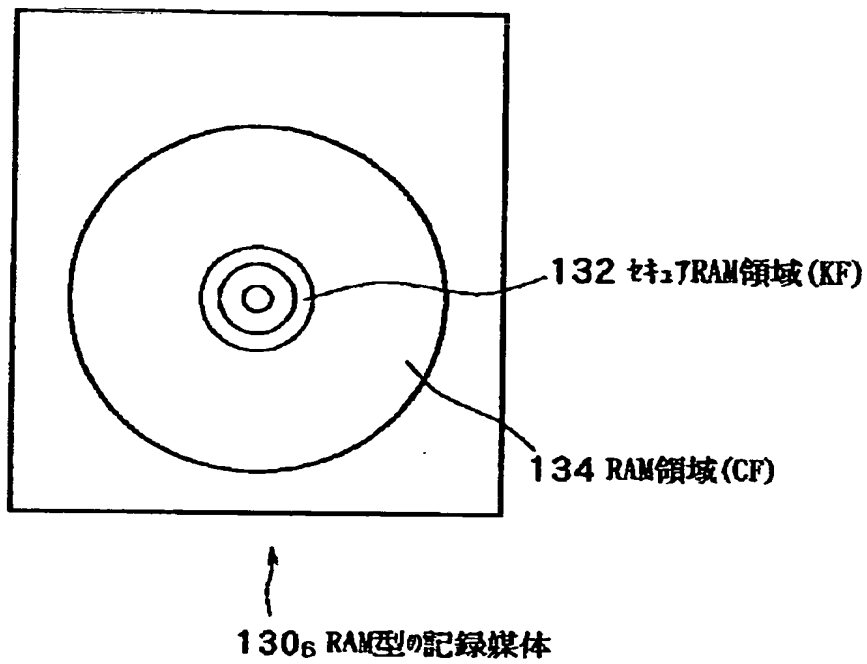
【図 1 5】



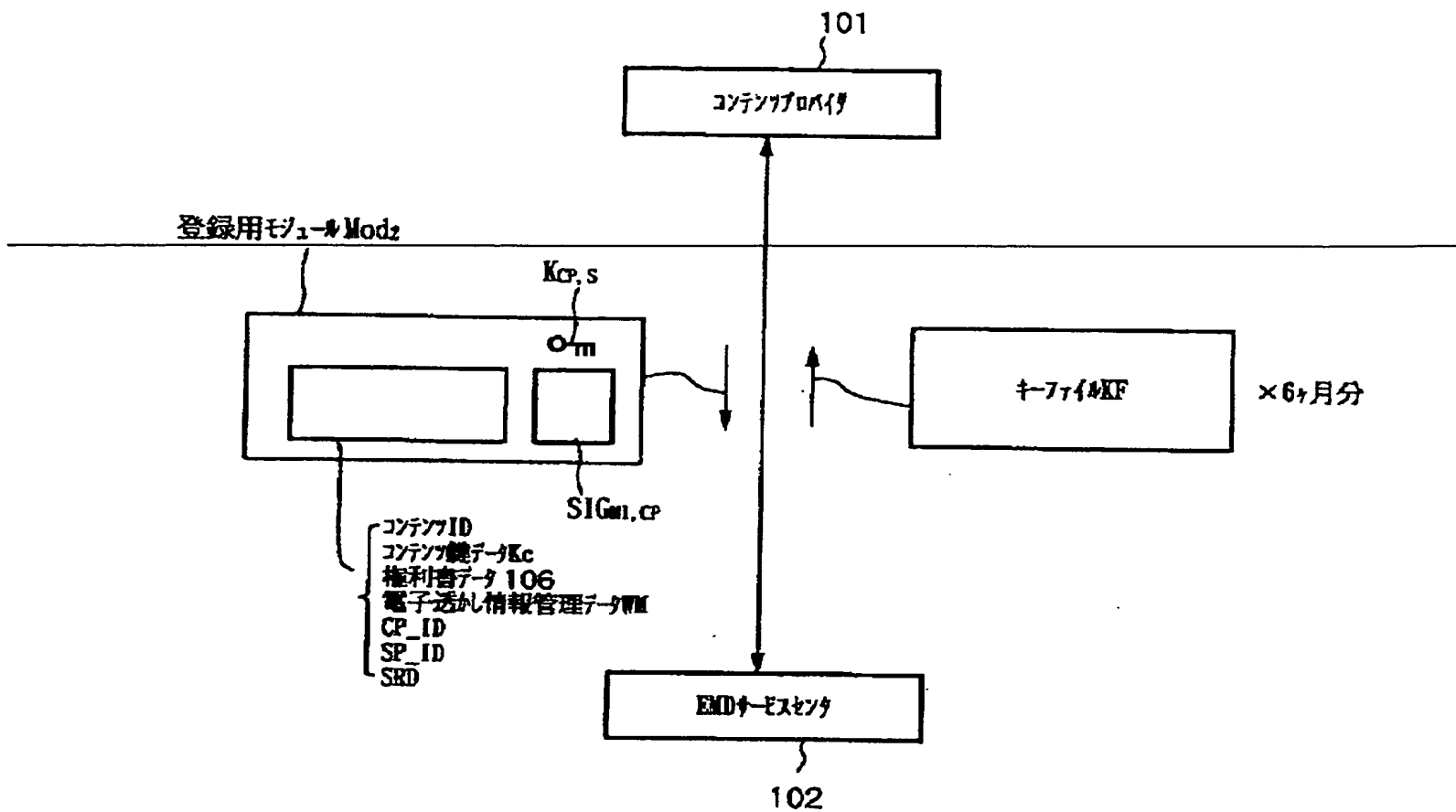
【図 16】



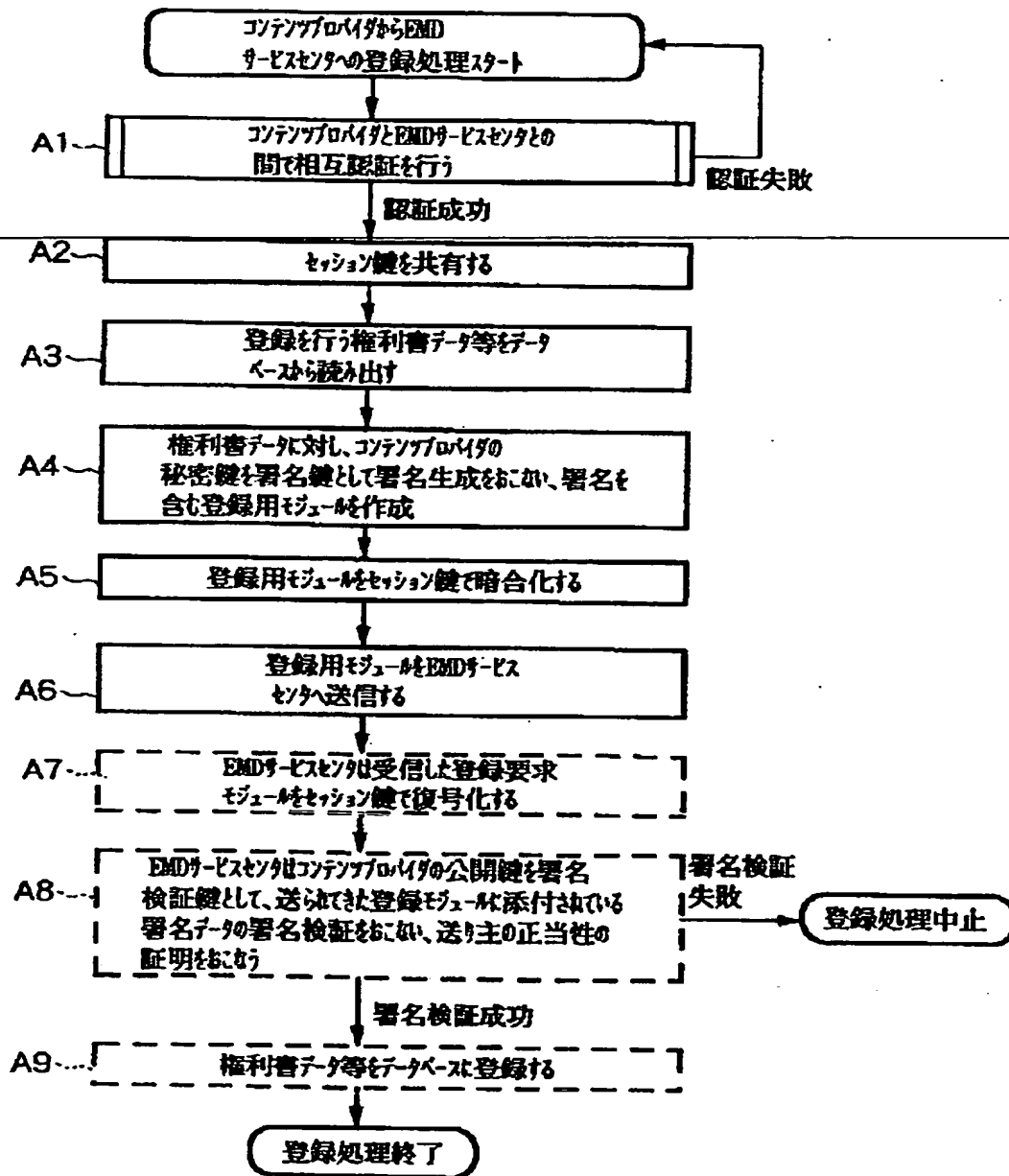
【図 17】



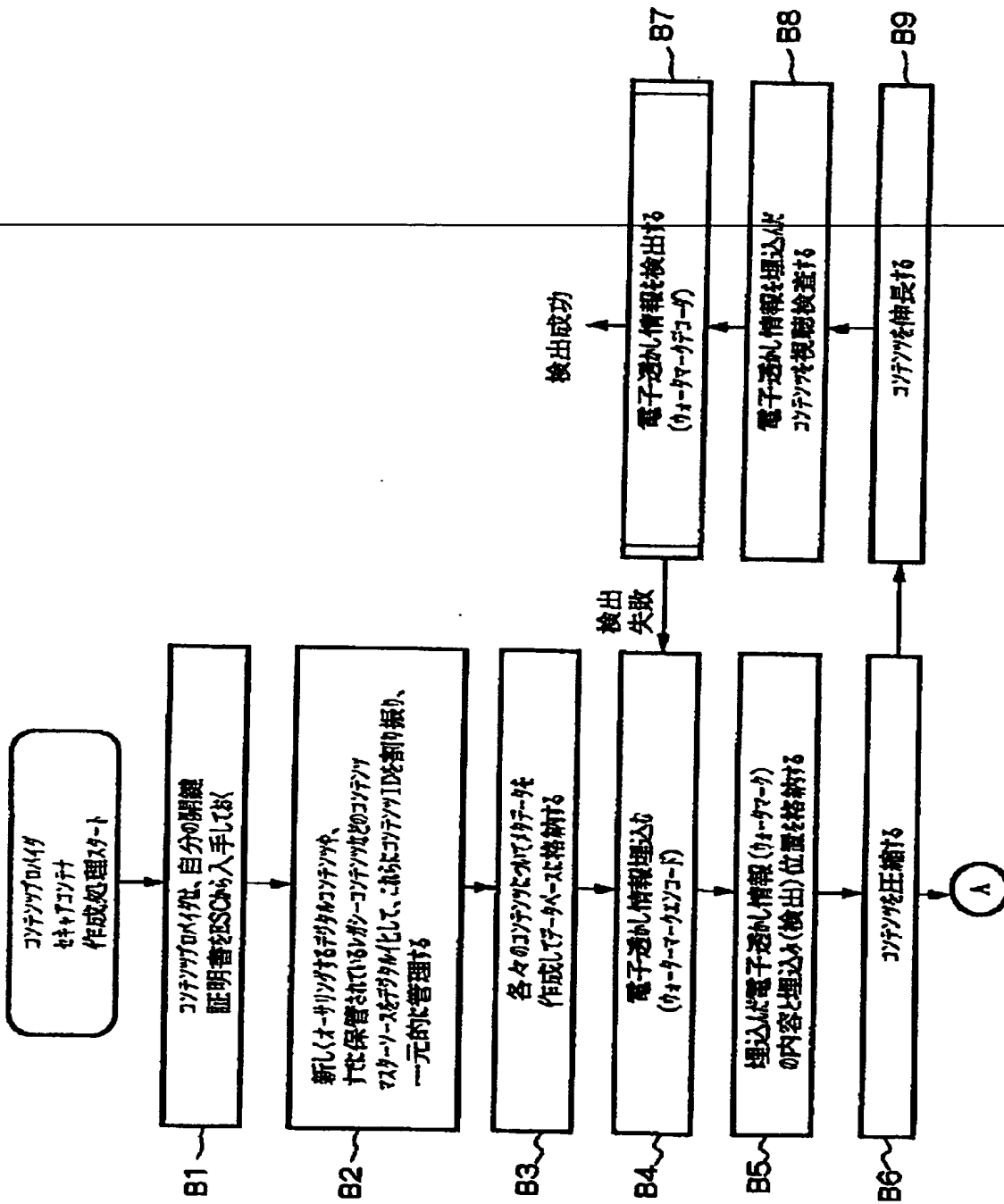
【図 18】



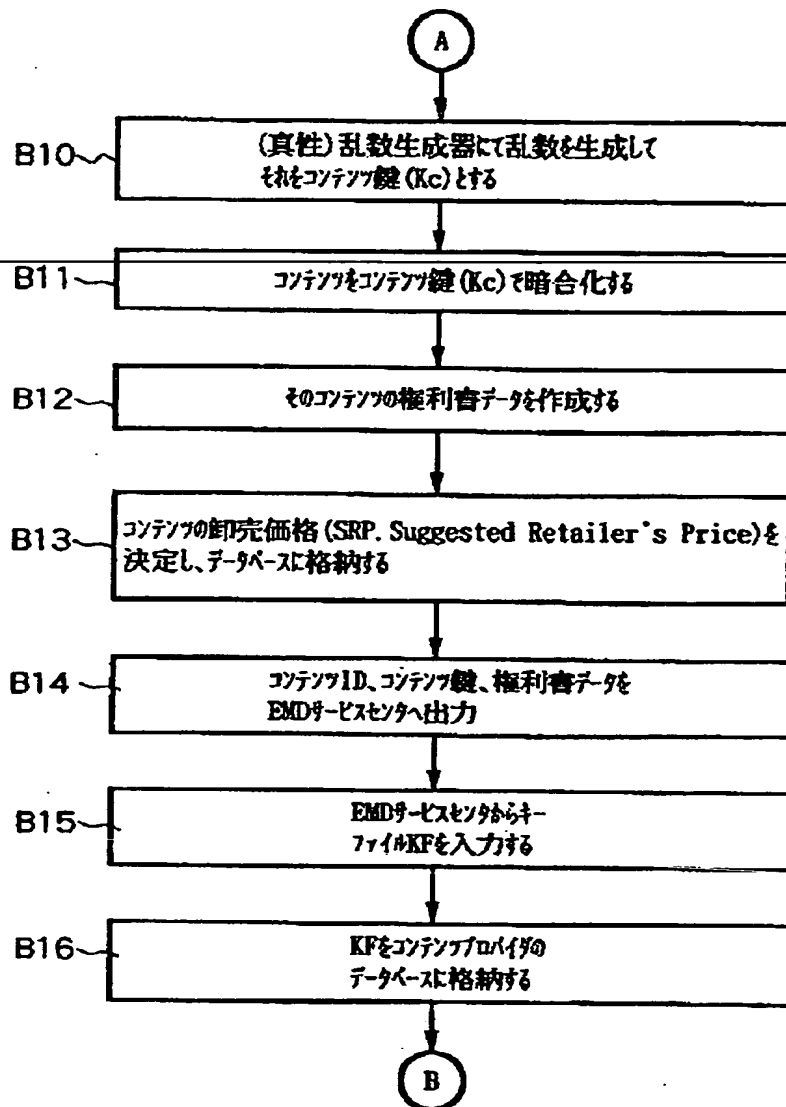
【図 19】



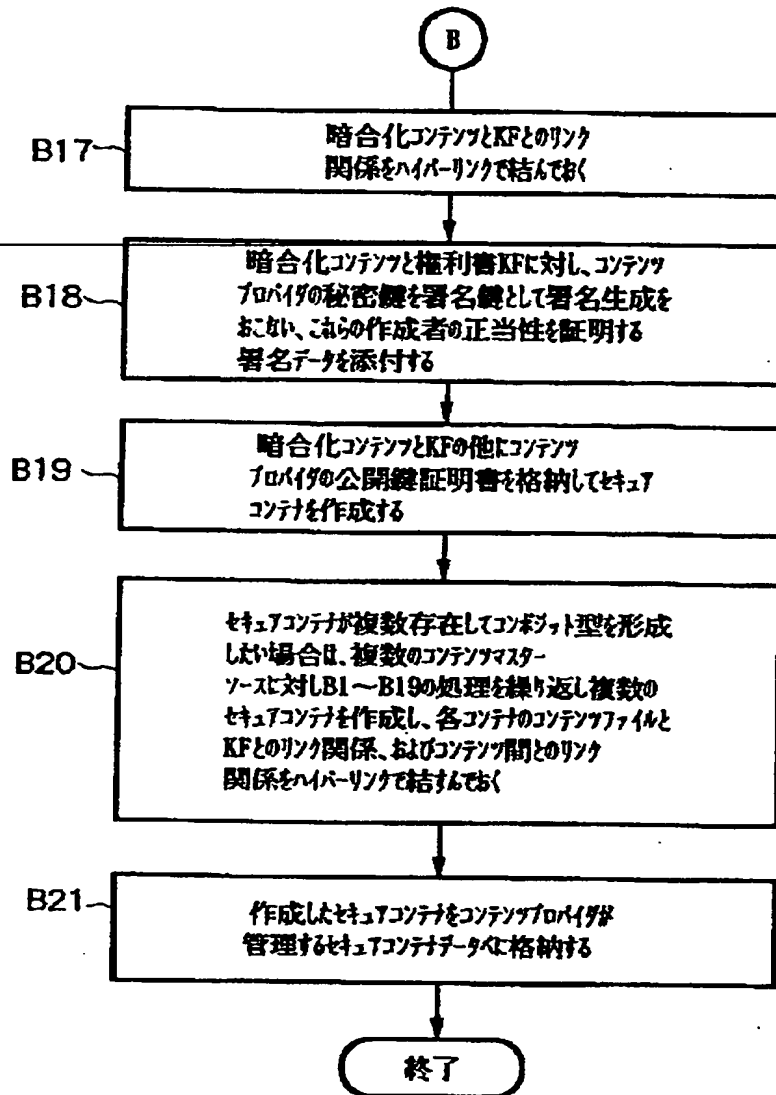
【図 2 0】



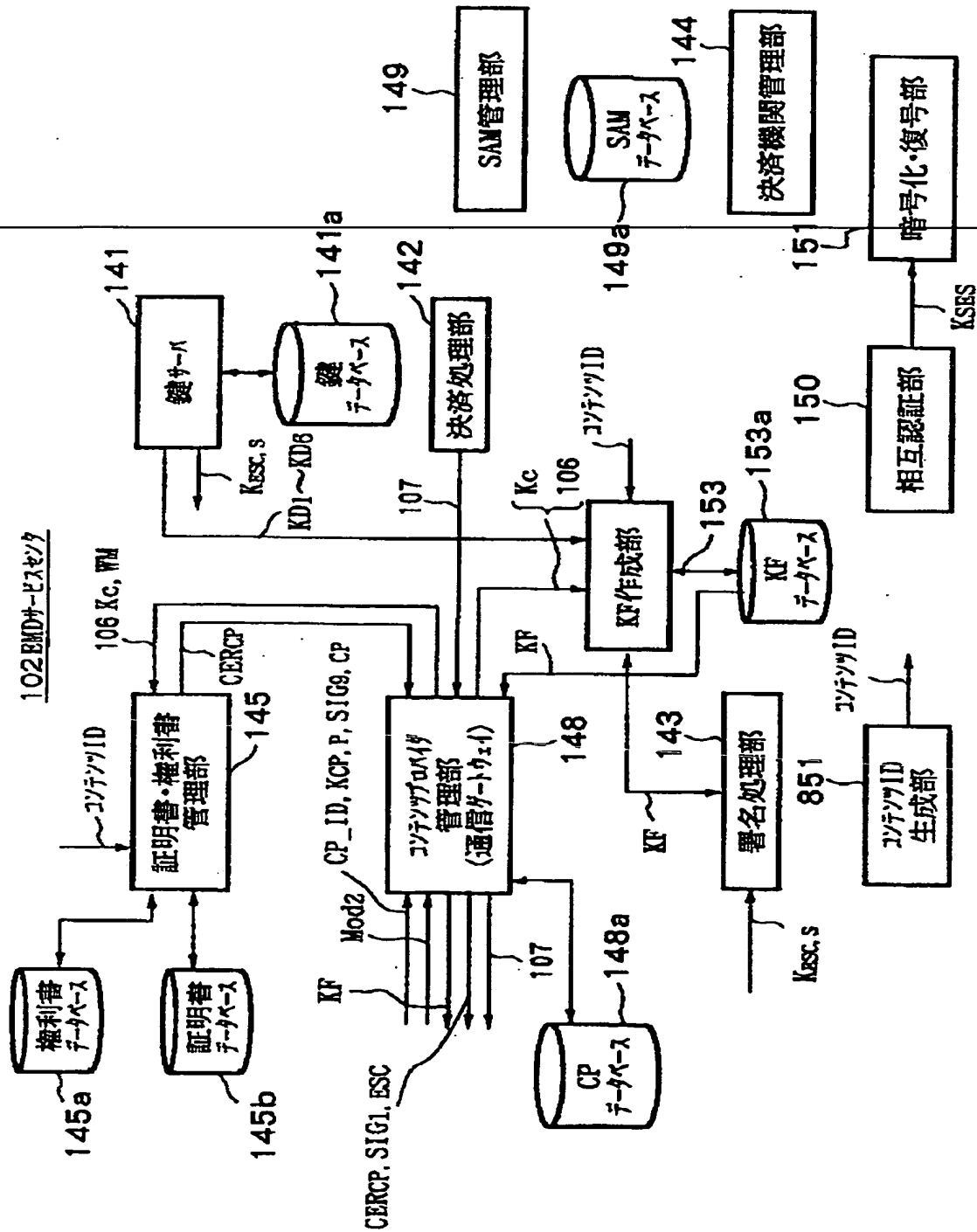
【図 21】



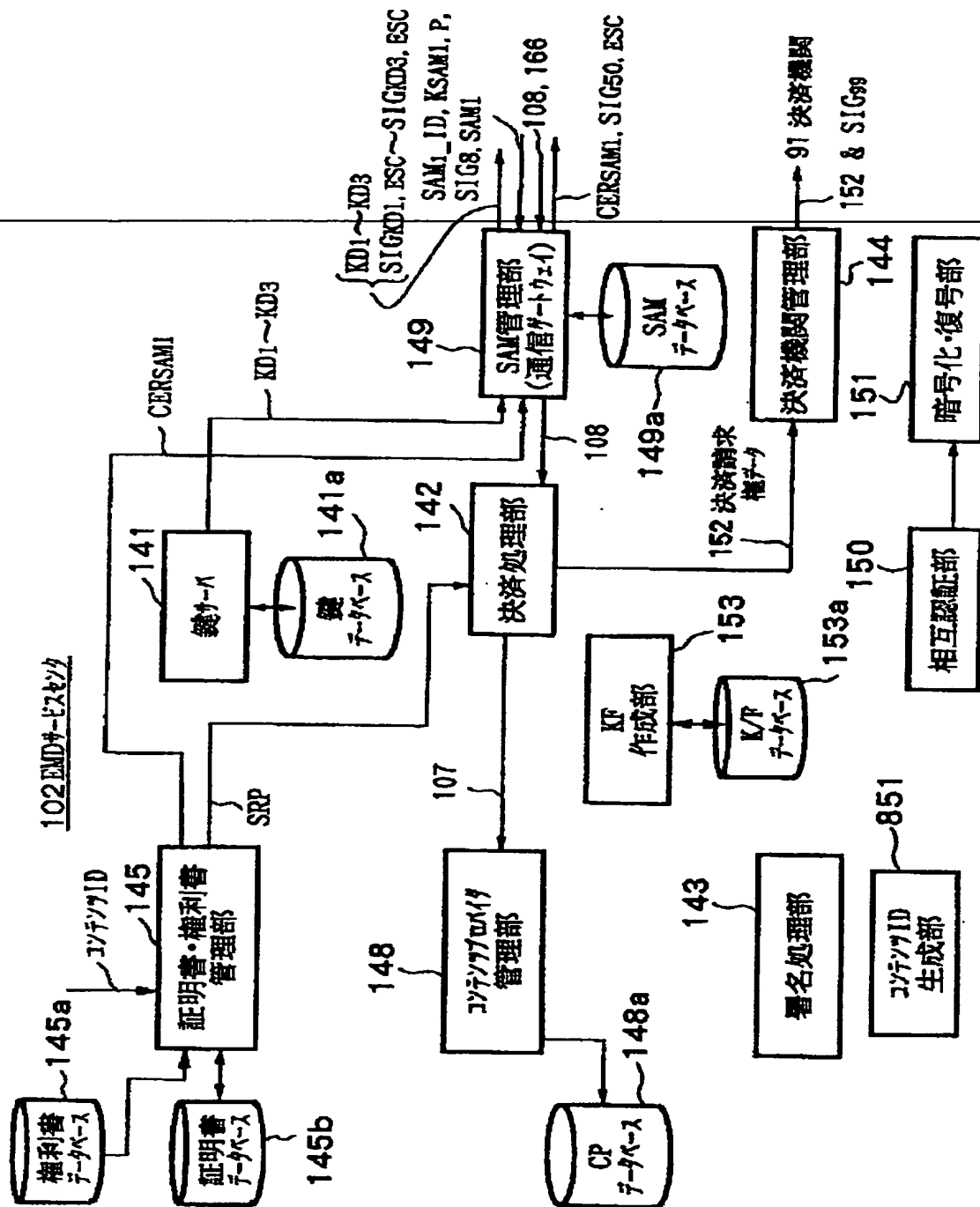
【図 2 2】



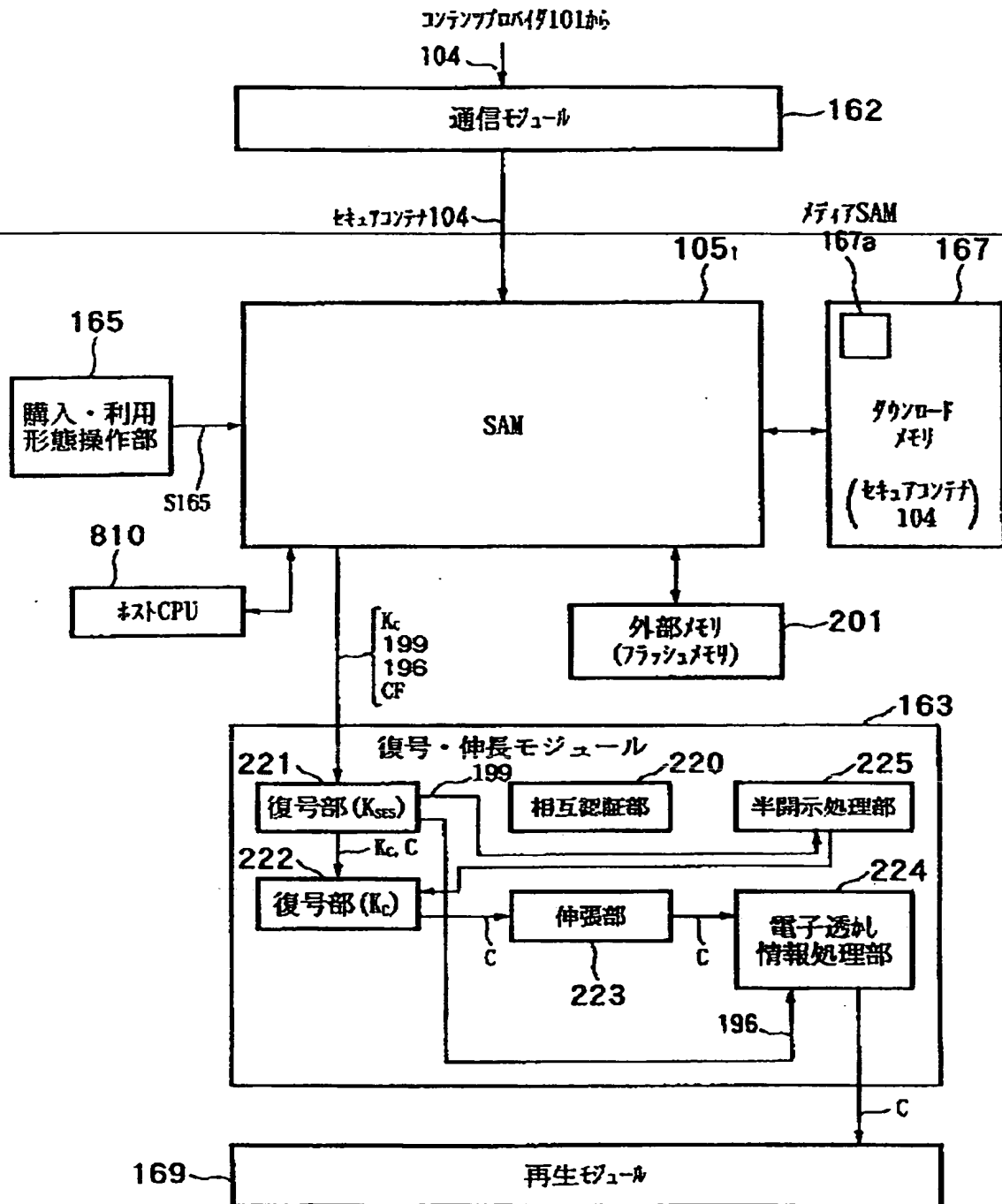
【図 23】



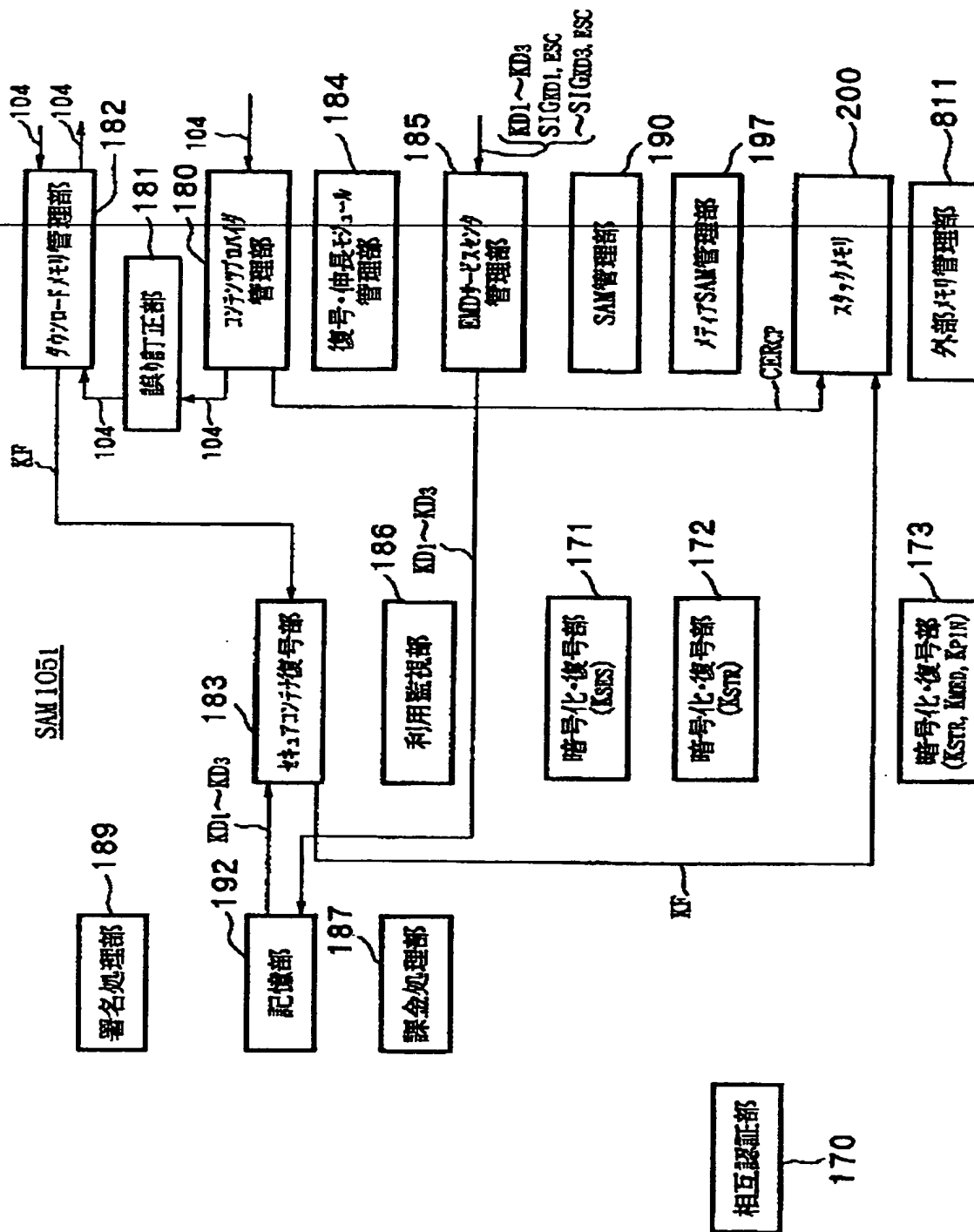
【図 2 4】



【図 25】



【図 2 6】



【図 27】

外部メモリ201に記憶されるデータ

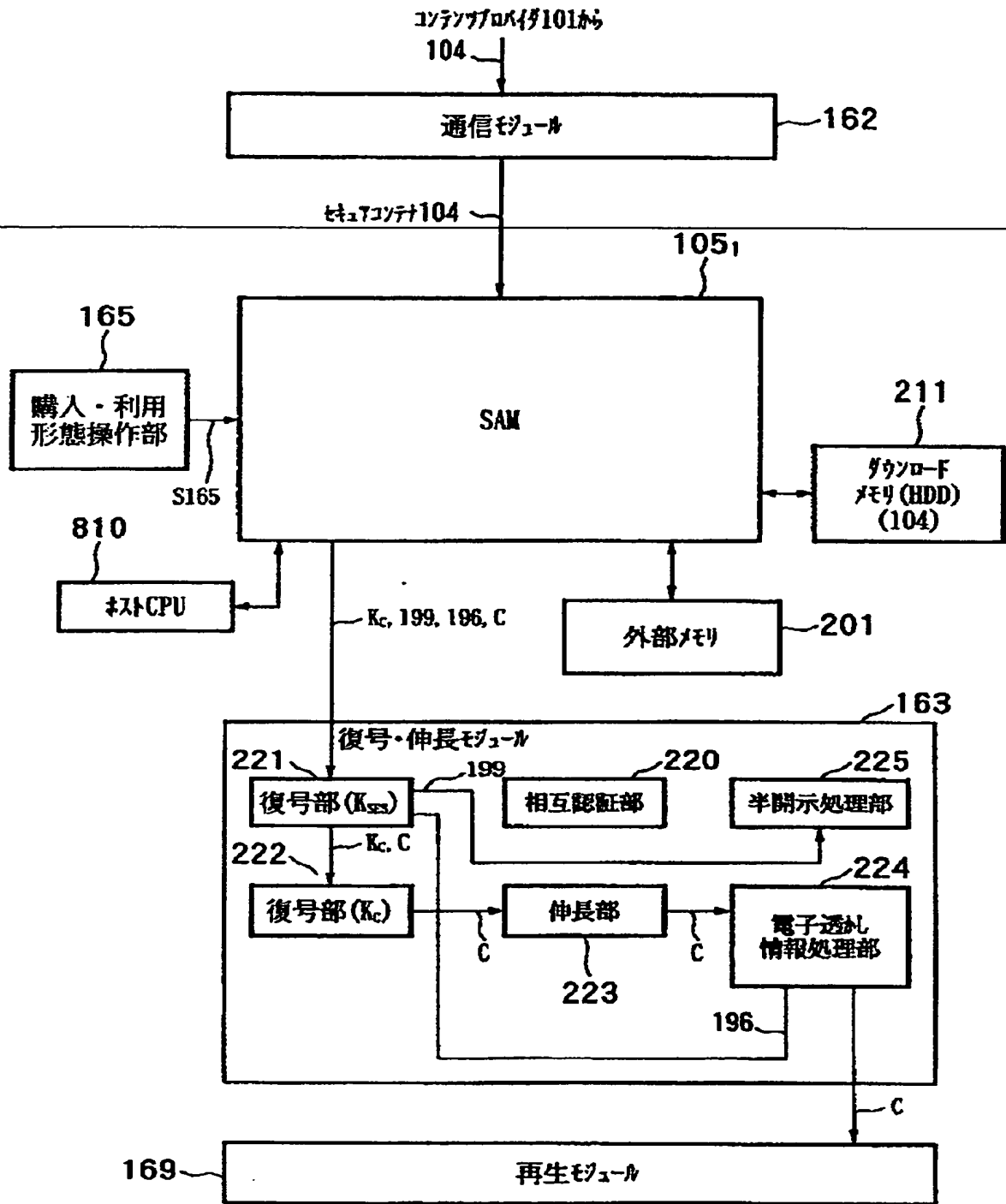
利用履歴データ108
SAM登録リスト

【図 28】

スタックメモリ200に記憶されるデータ

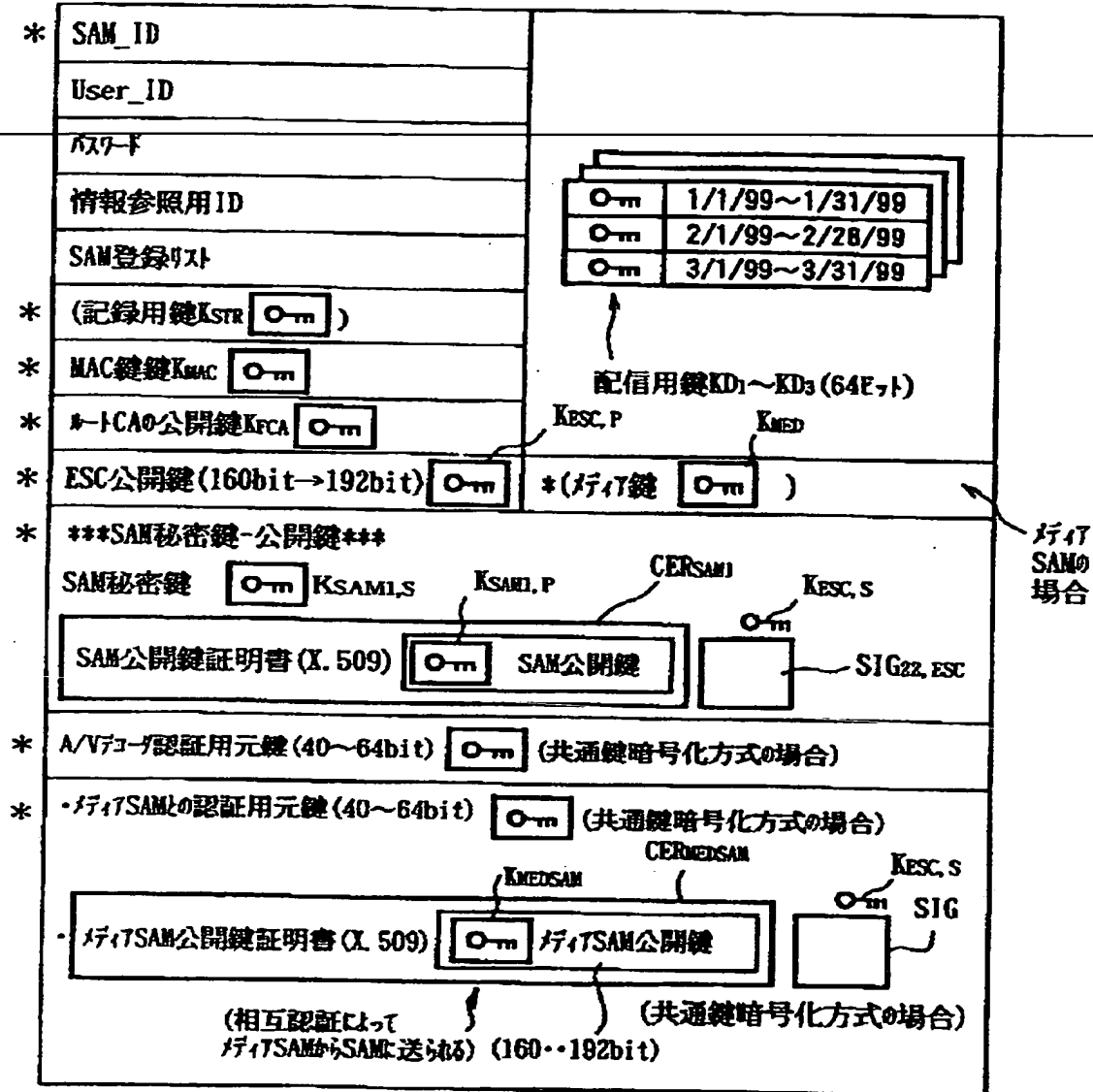
コンテンツ鍵データKc
権利書データ(UCP)106
記憶部(フラッシュメモリ)192のロック鍵データKLoc
コンテンツプロバイダ101の公開鍵証明書CERcp
利用制御情状態データ(UCS)166
SAMプログラム・ダウンロード・コンテンツSD₁～SD₃

【図 29】

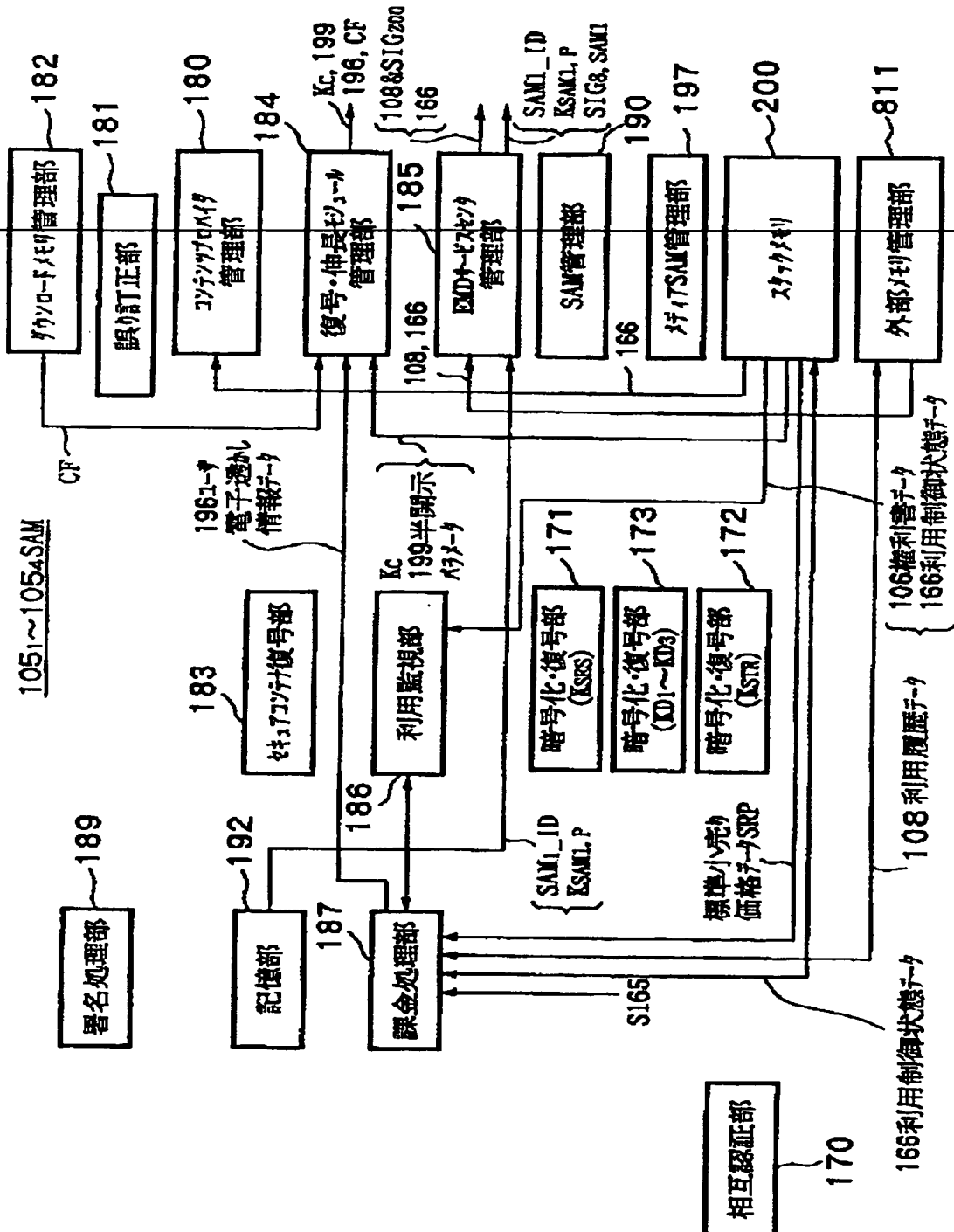


【図30】

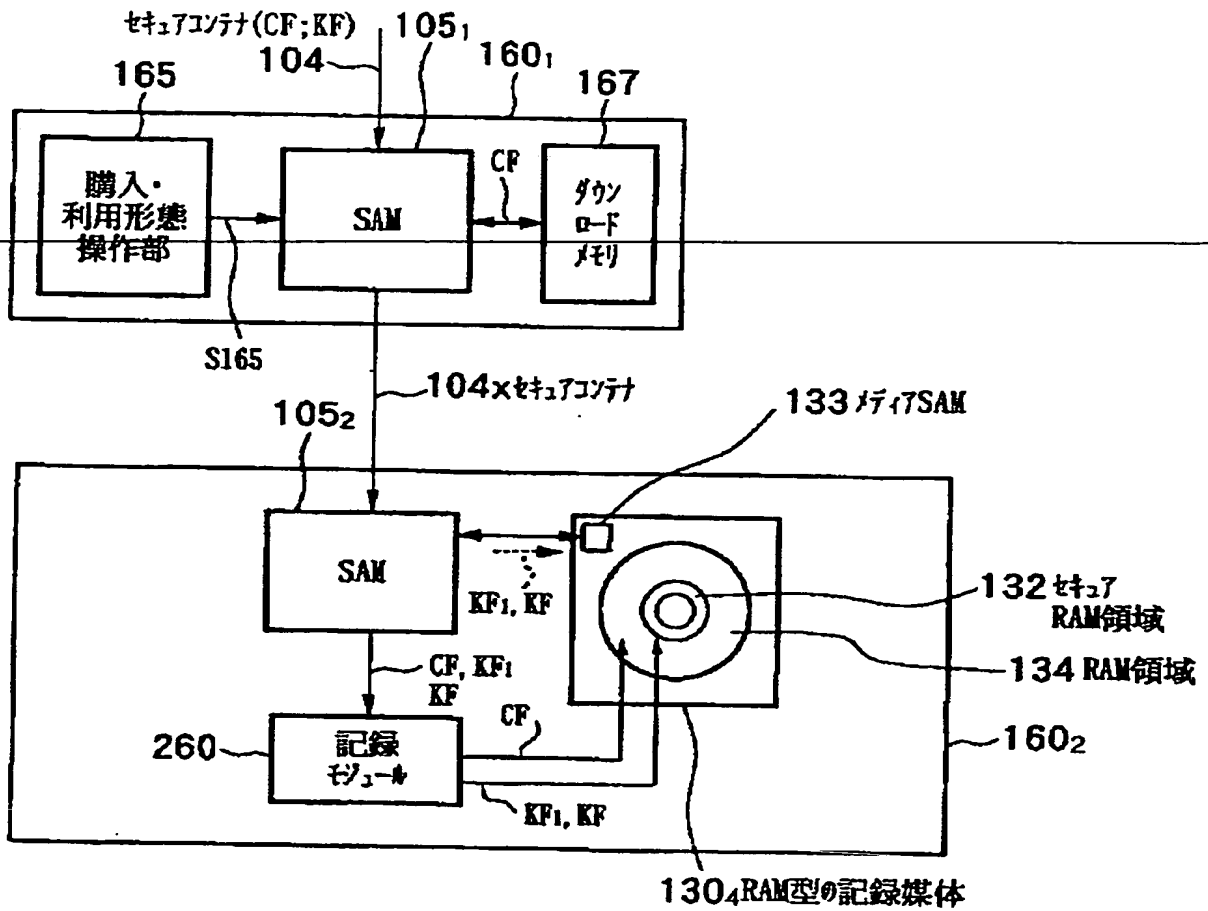
記憶部192に記憶されるデータ



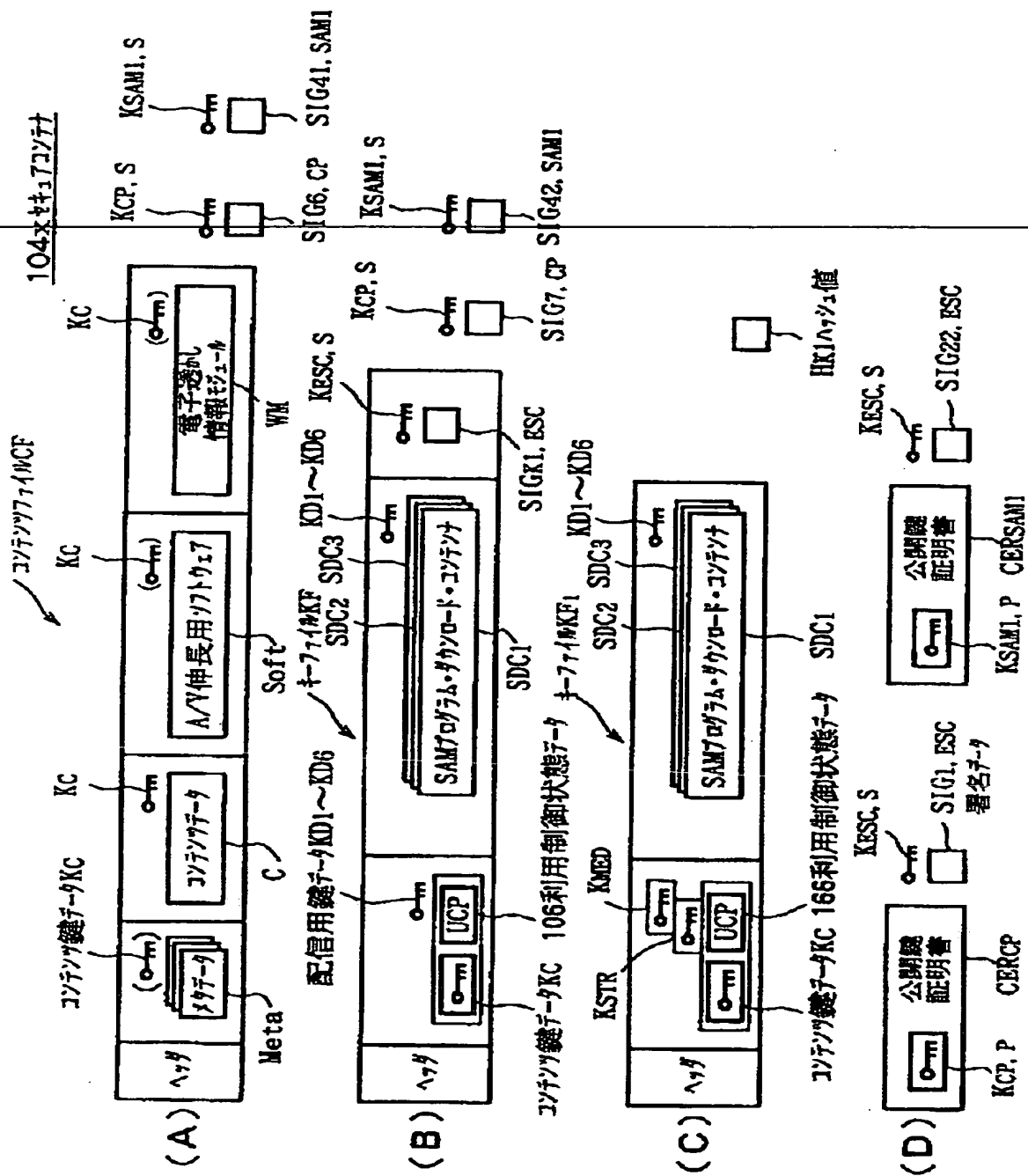
【図 3 1】



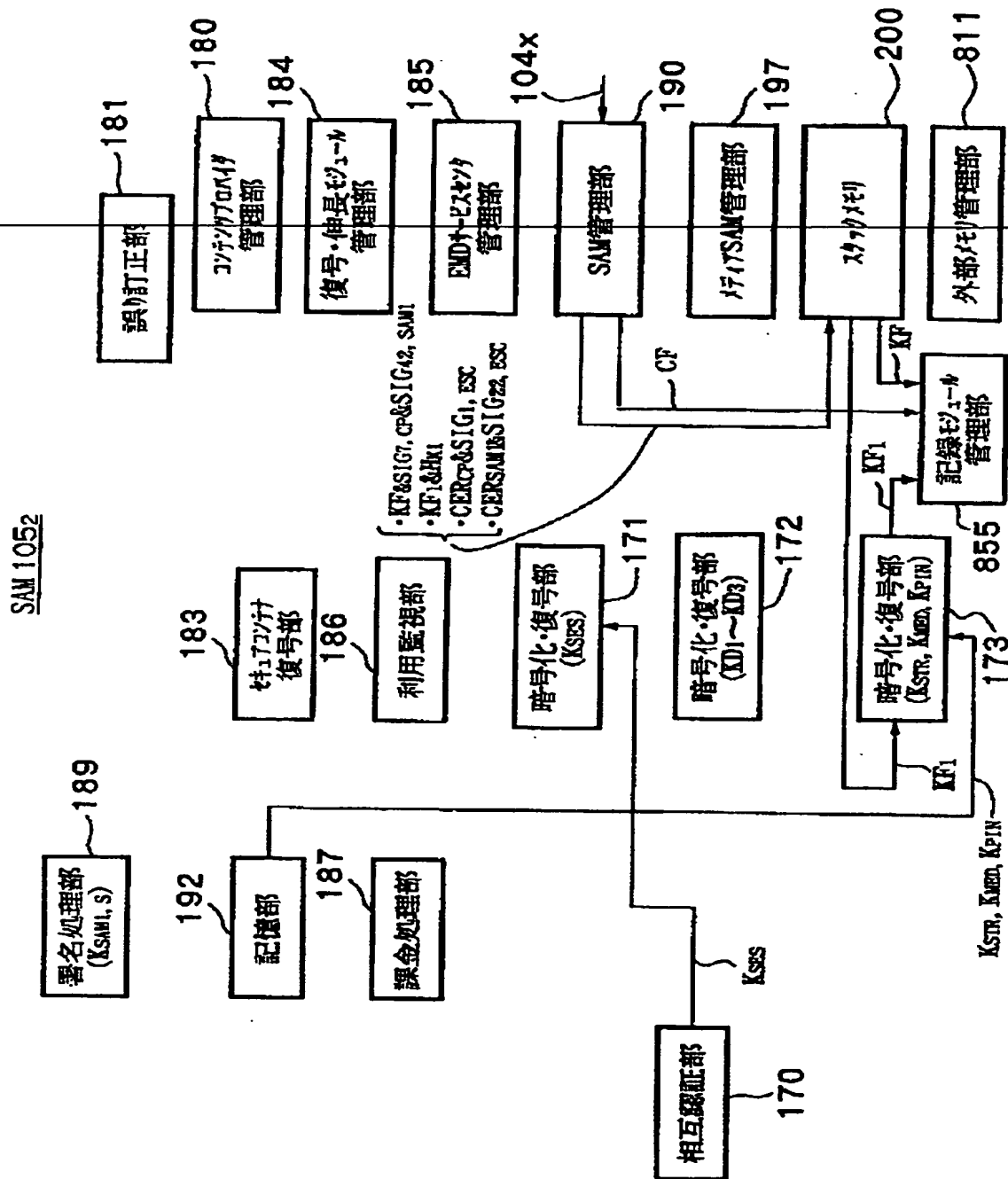
【図 3 2】



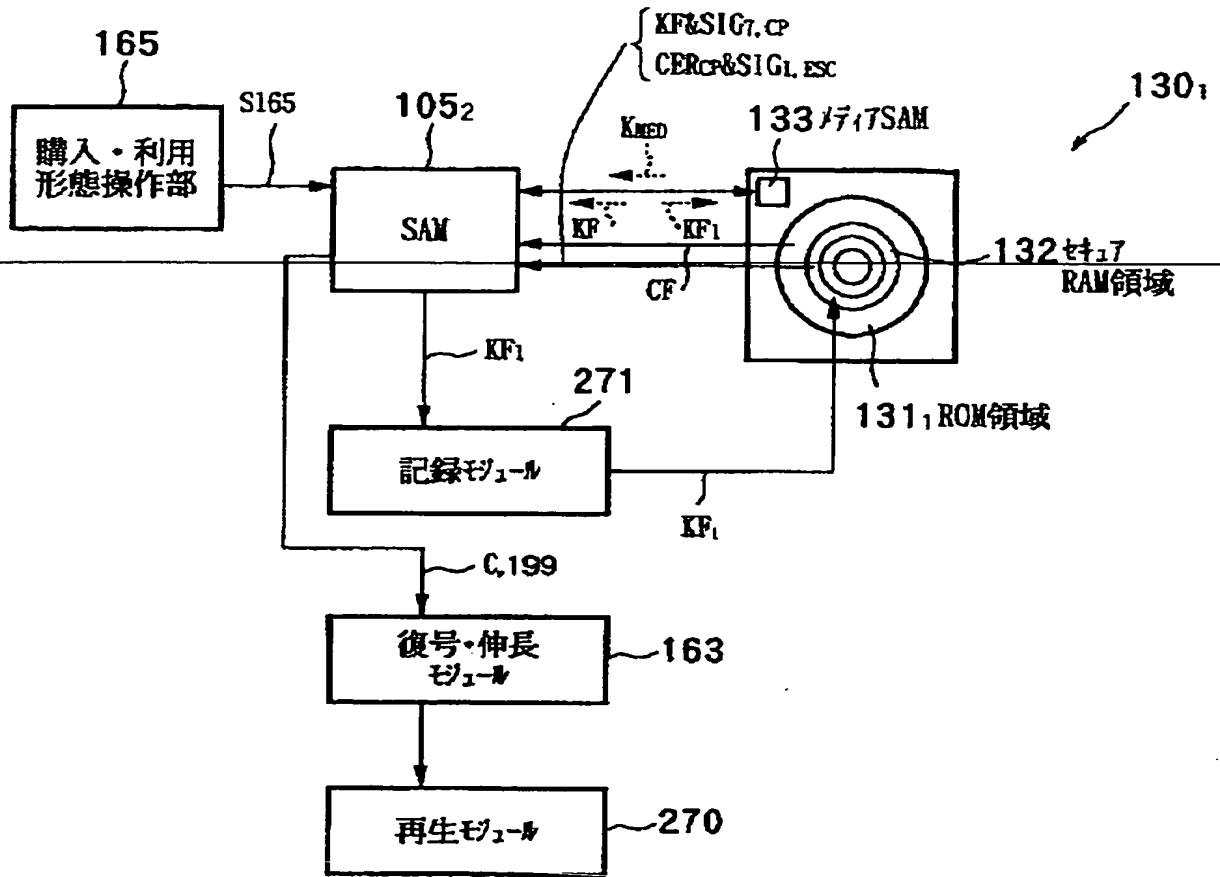
【図 3 4】



【図 3 5】

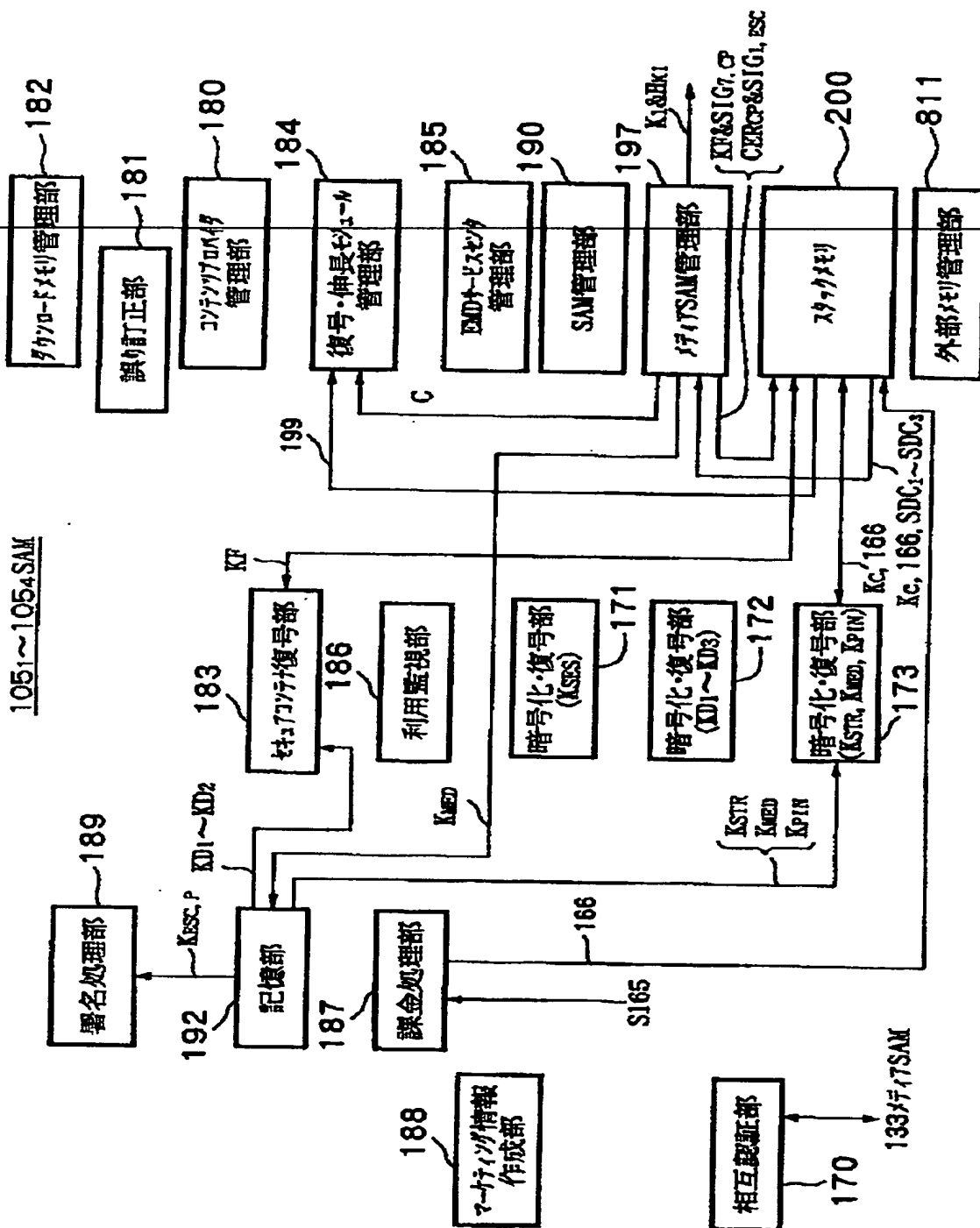


【図 3 6】

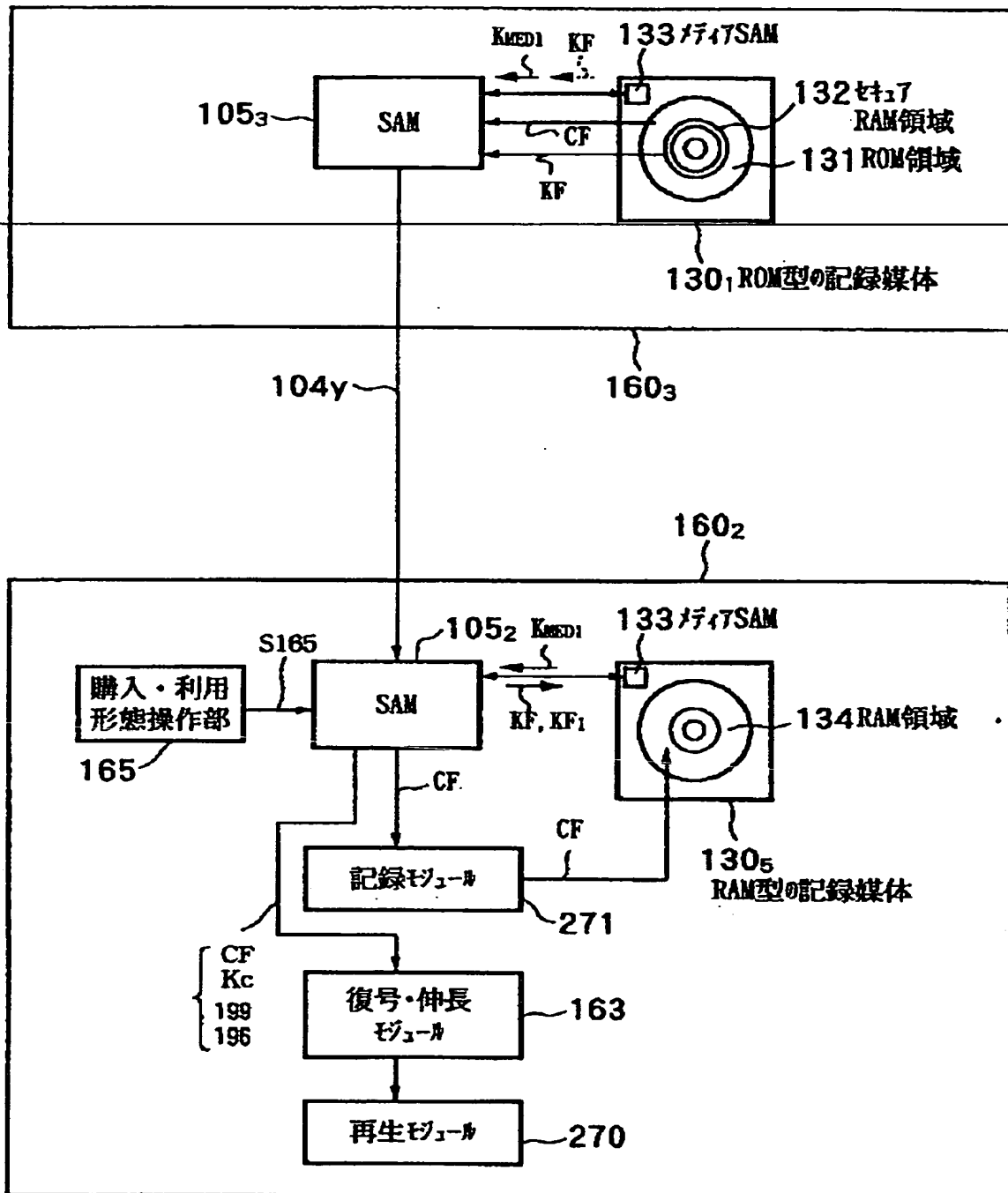


160₂

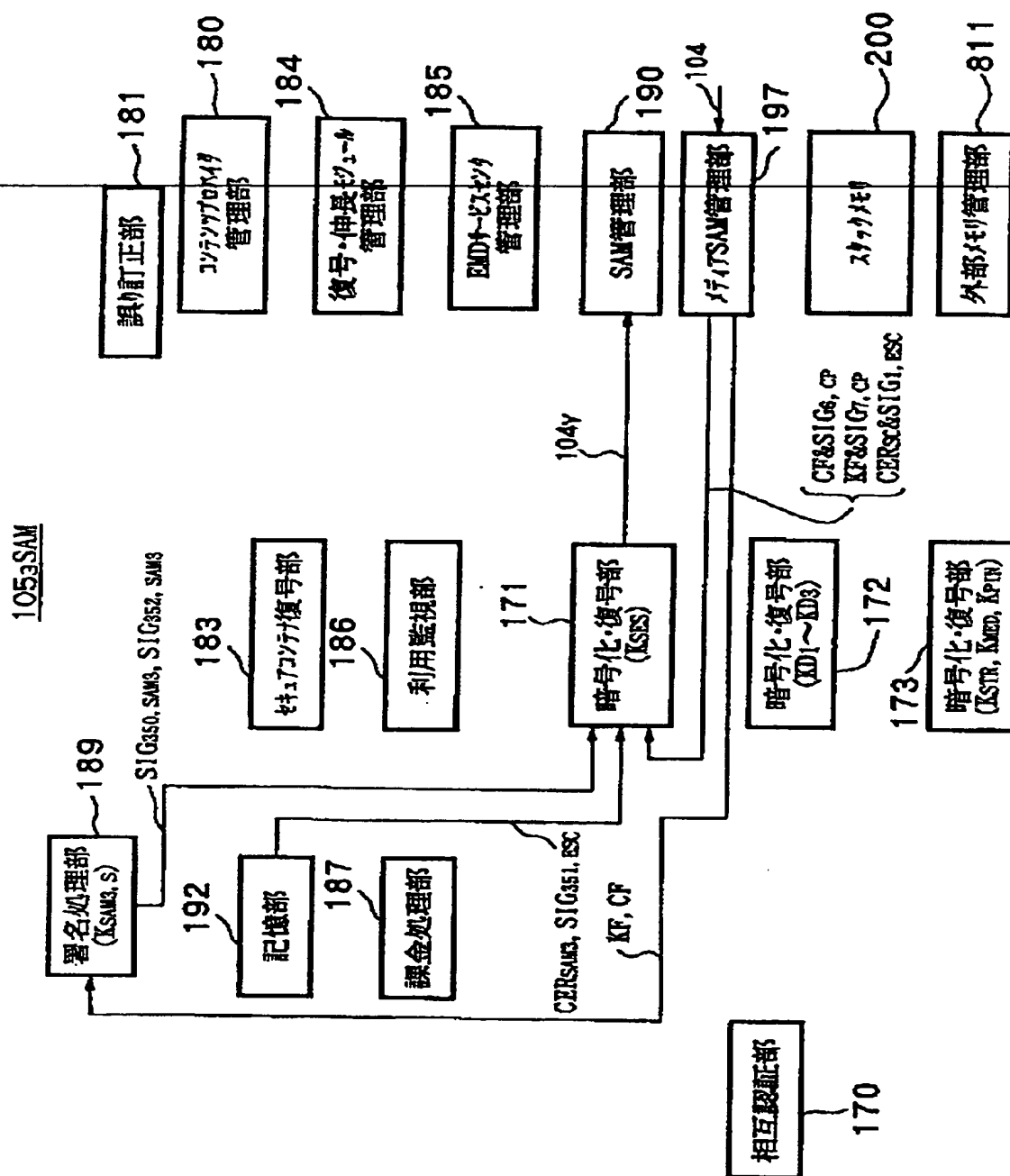
【图 3 7】



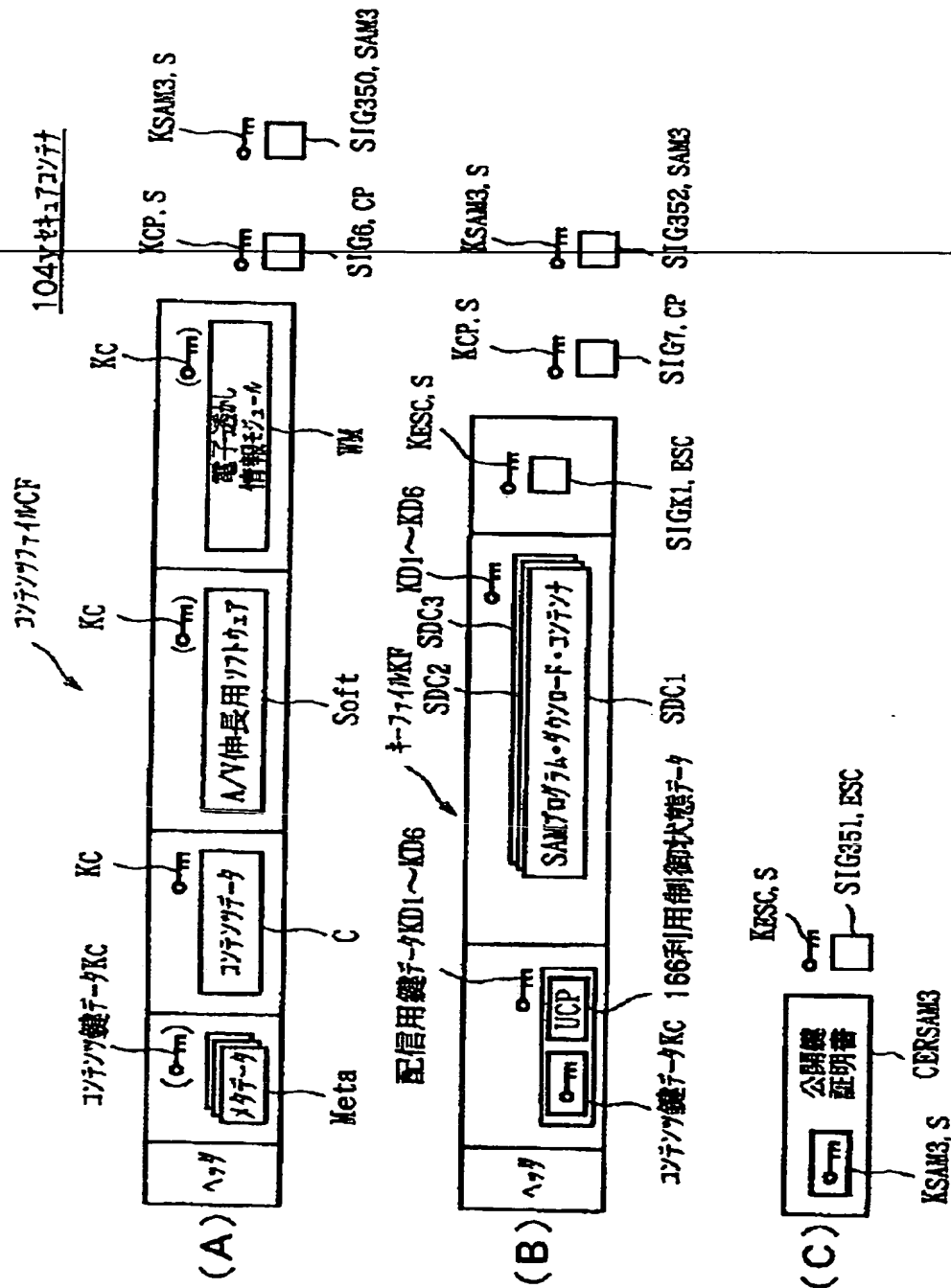
【図 38】



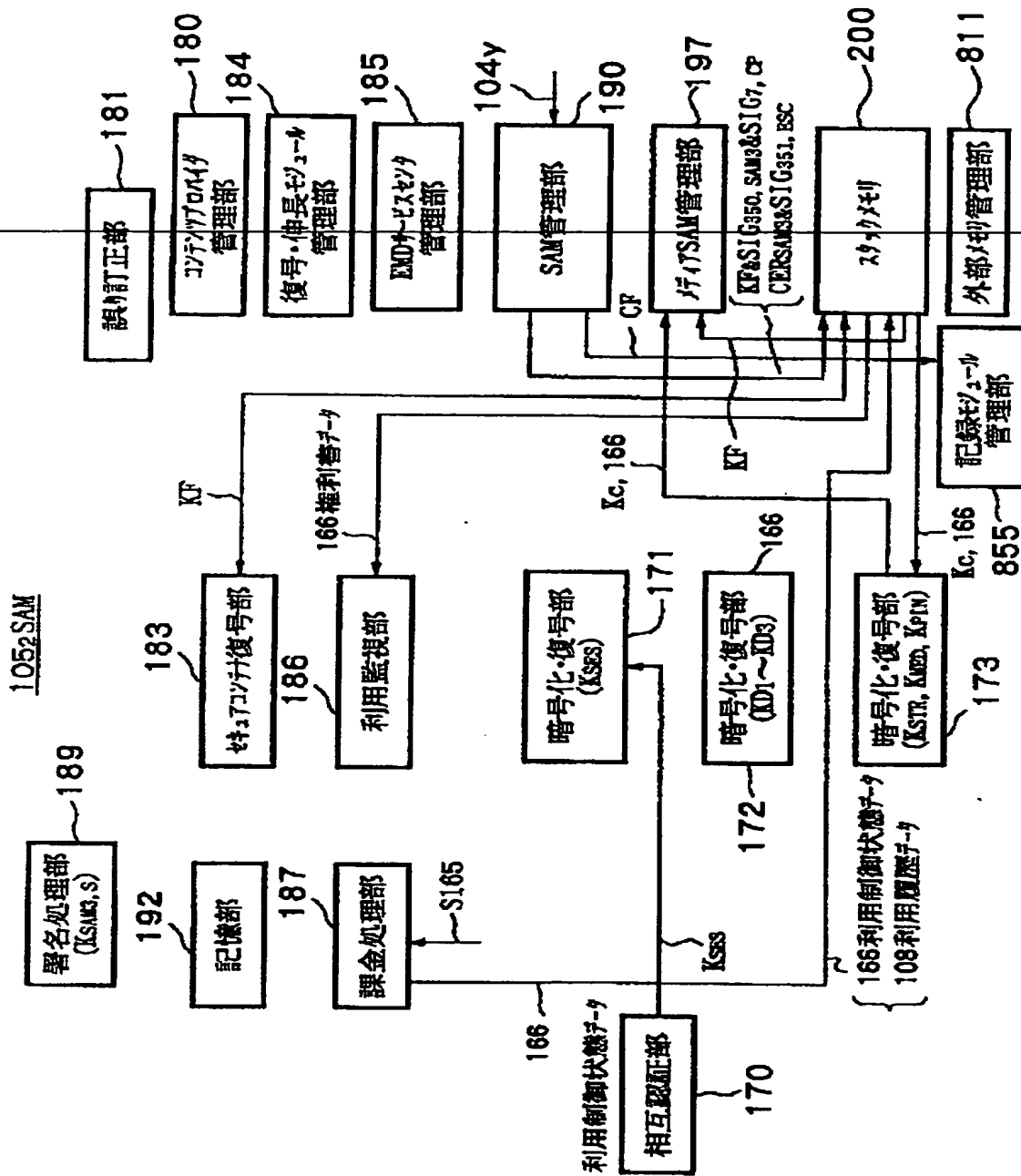
【図 39】



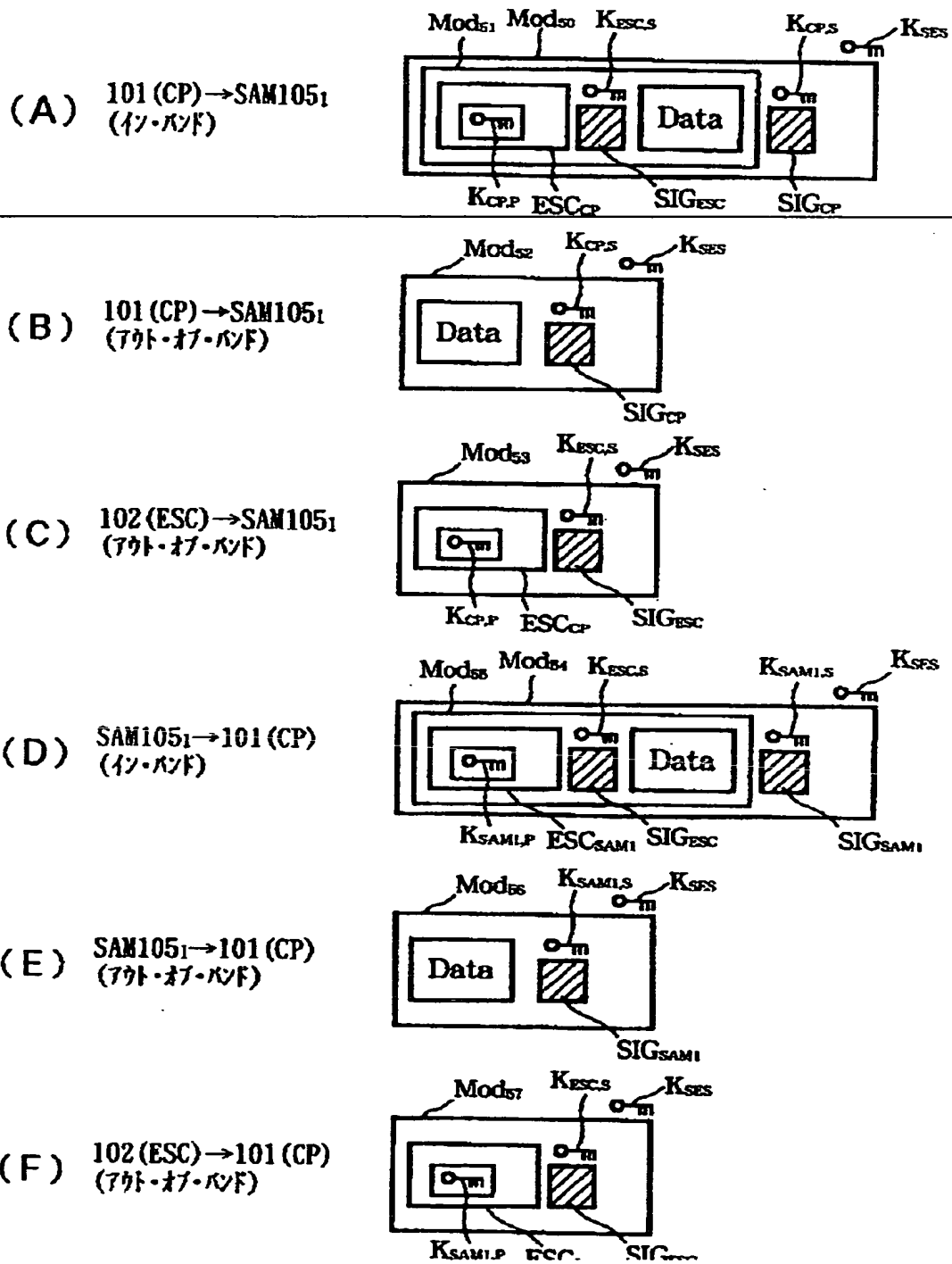
【図 40】



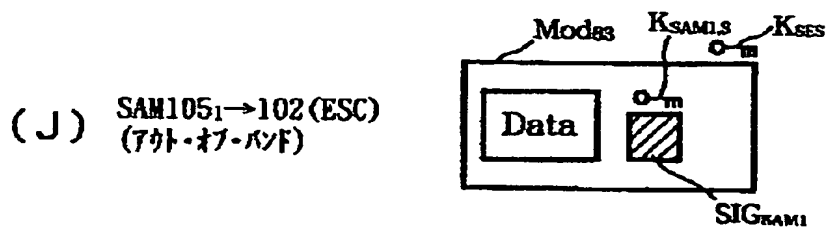
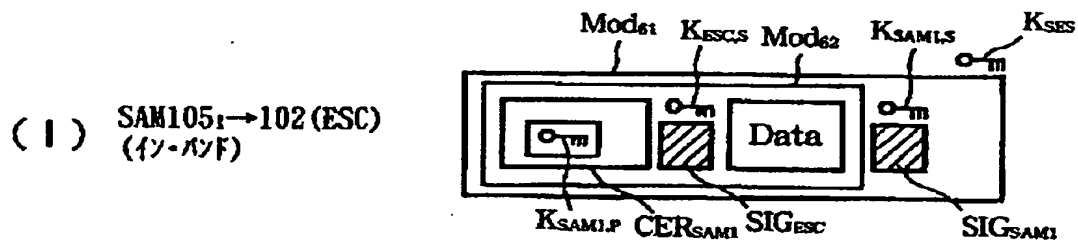
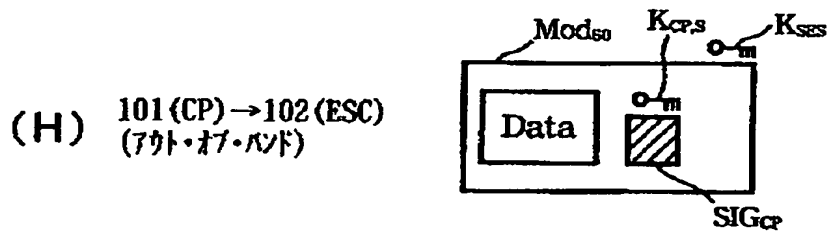
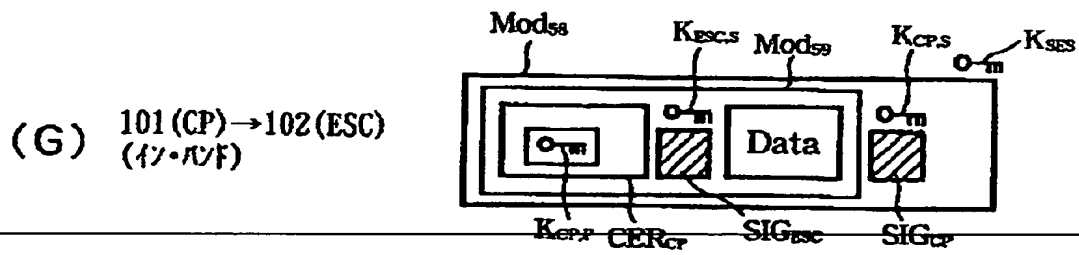
【図 4 1】



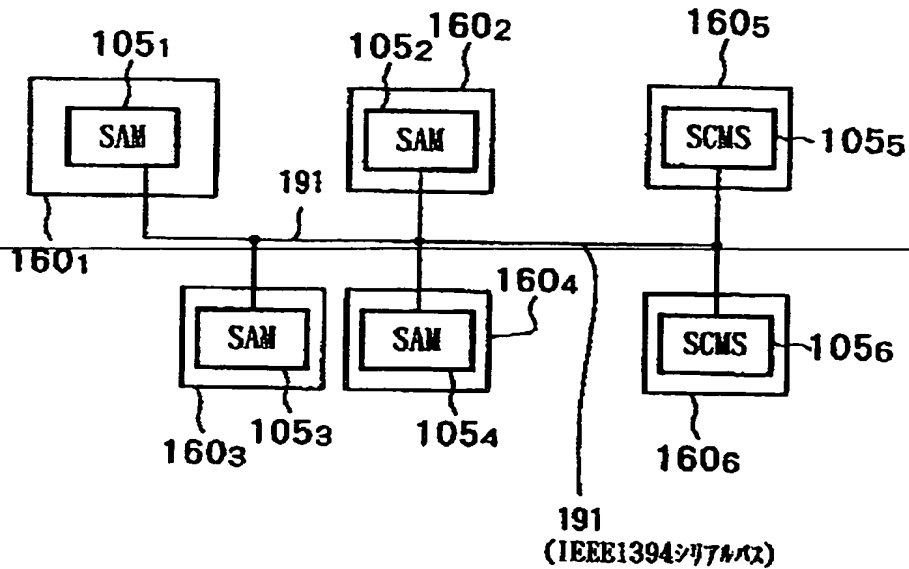
【図 4 2】



【図 4 3】

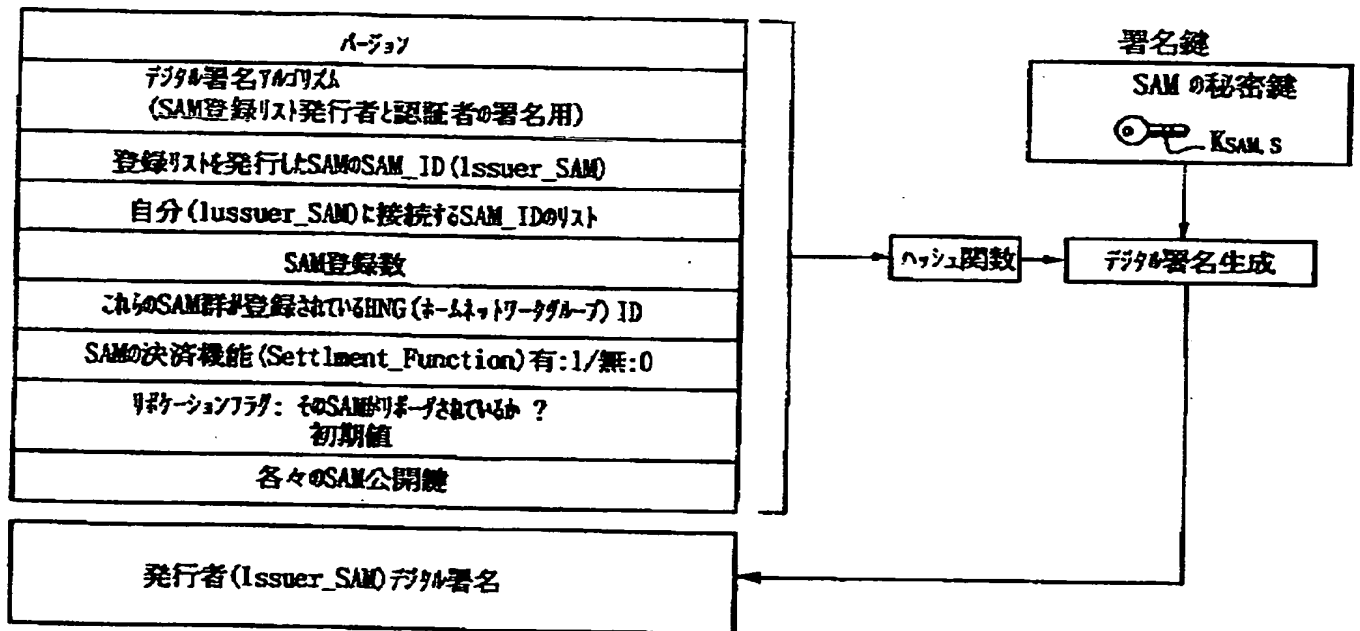


【図 4 4】



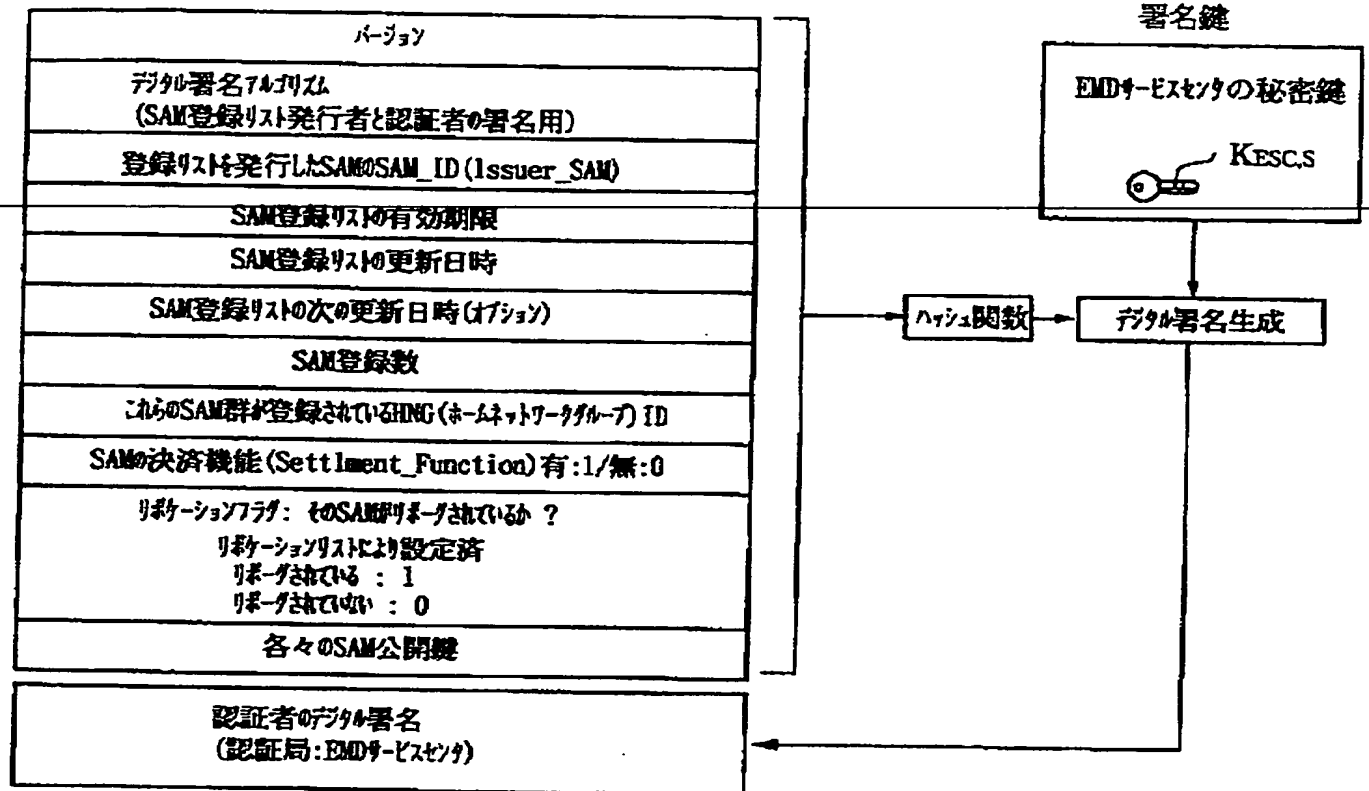
【図 4 5】

SAM登録リスト (SAM Registration List) (SAM作成)

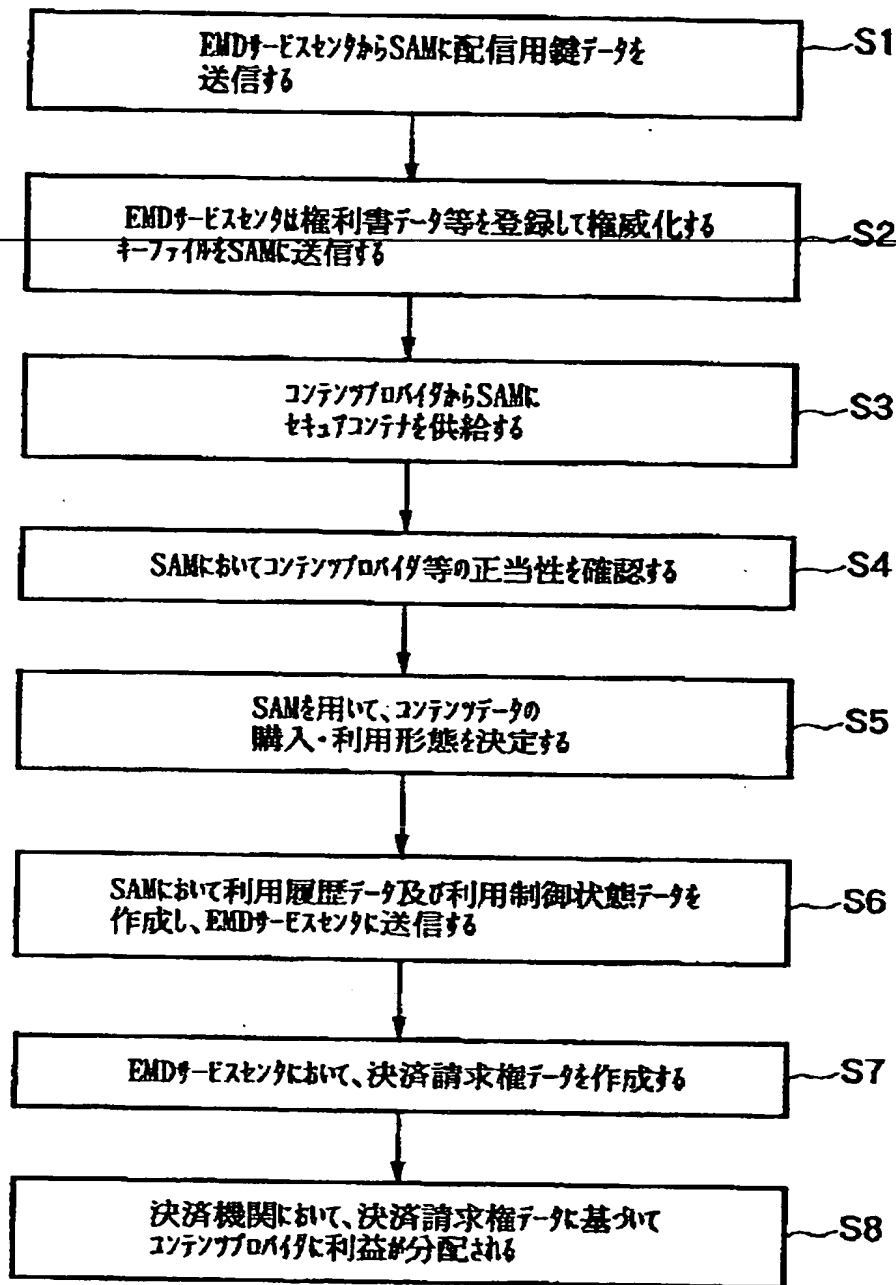


【図 4 6】

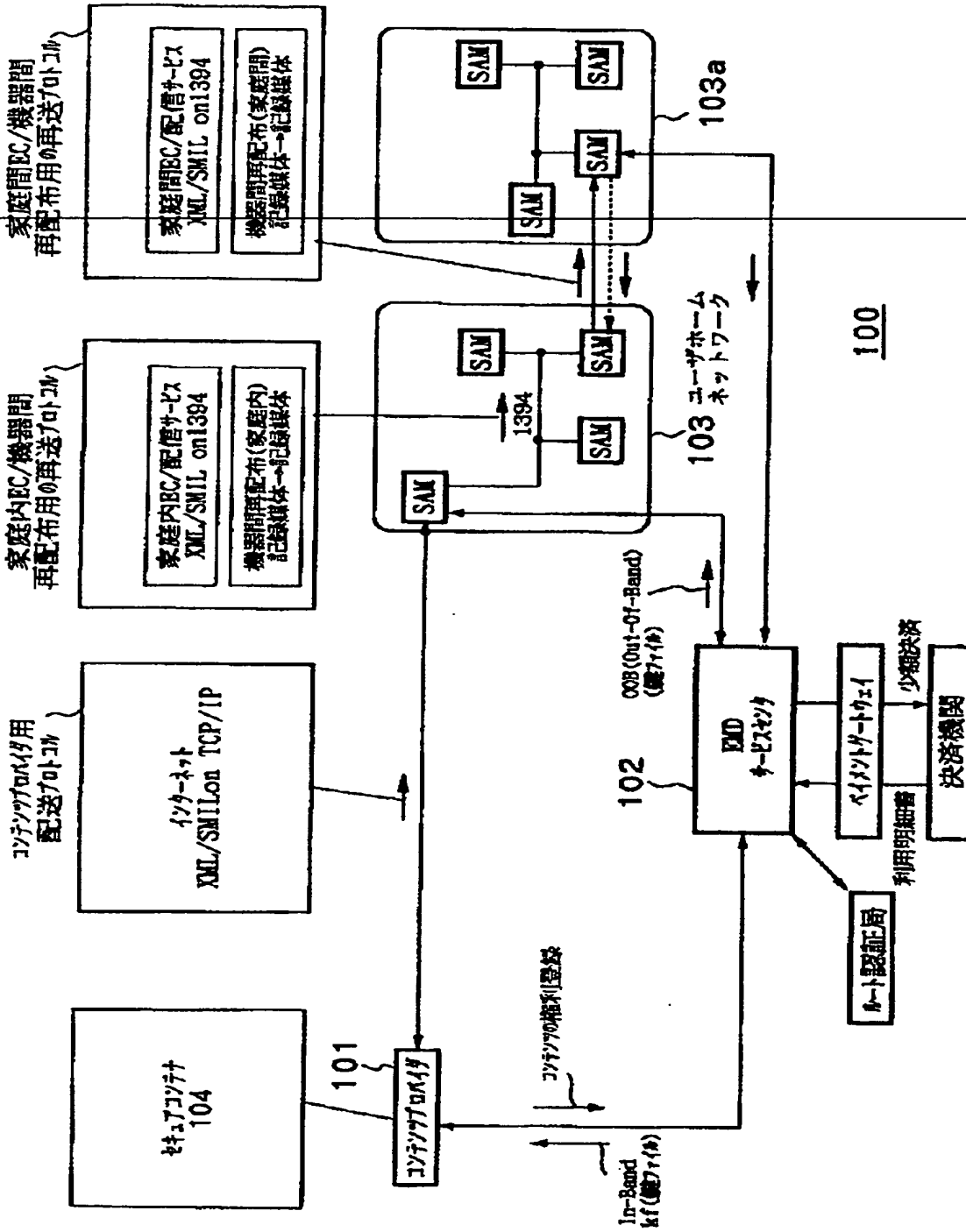
SAM登録リスト (EMDサービスセンタが作成)



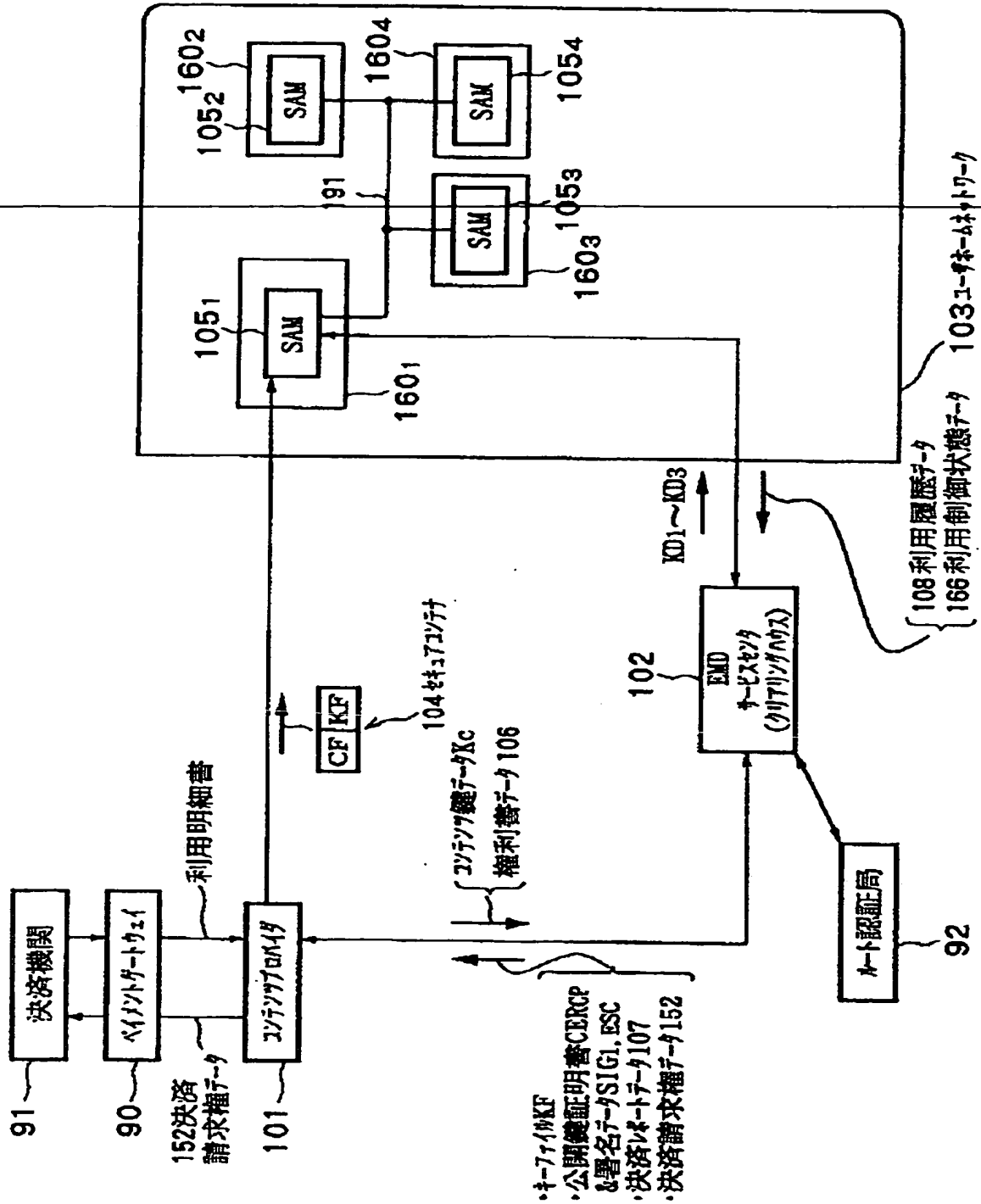
【図 4 7】



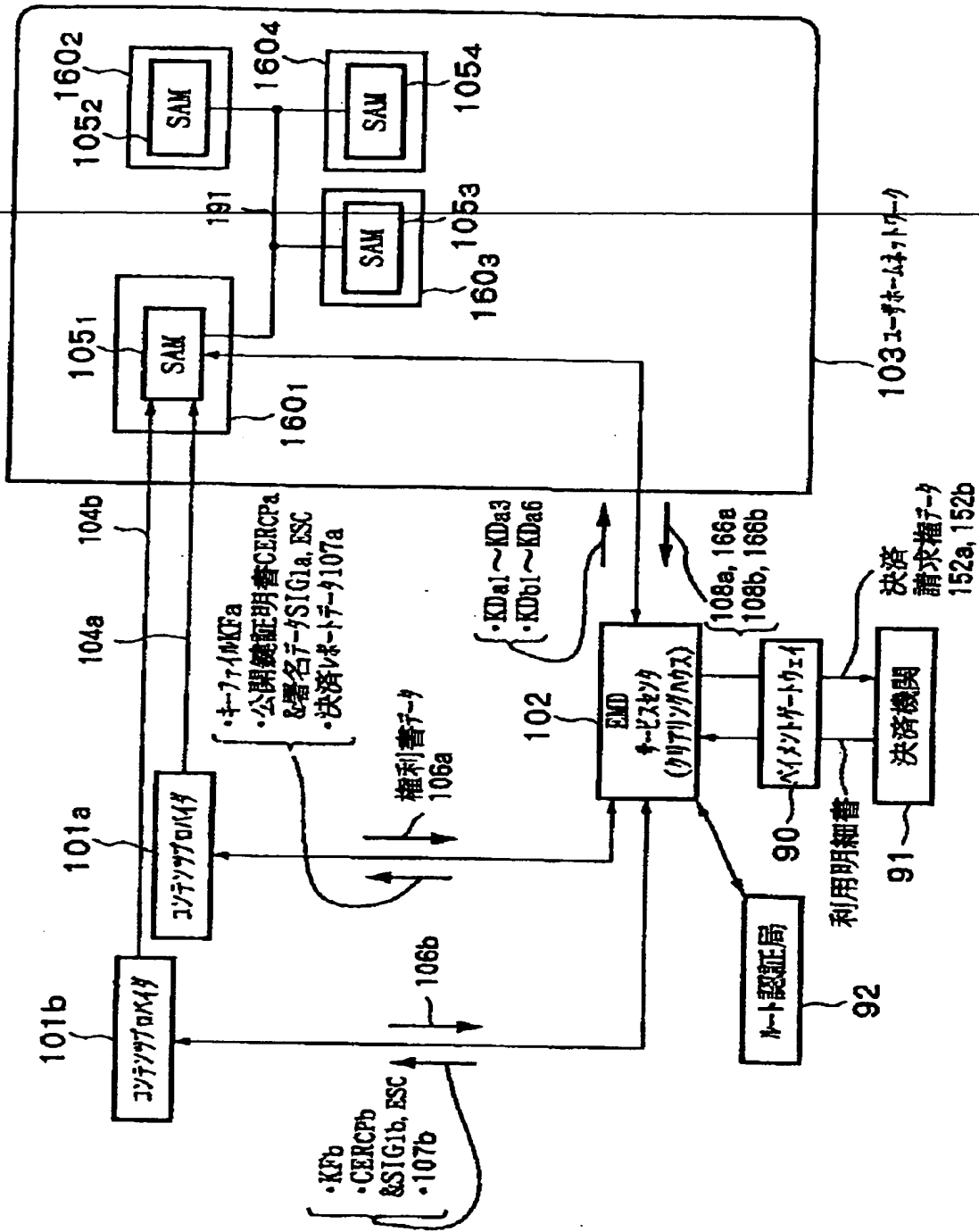
【図 48】



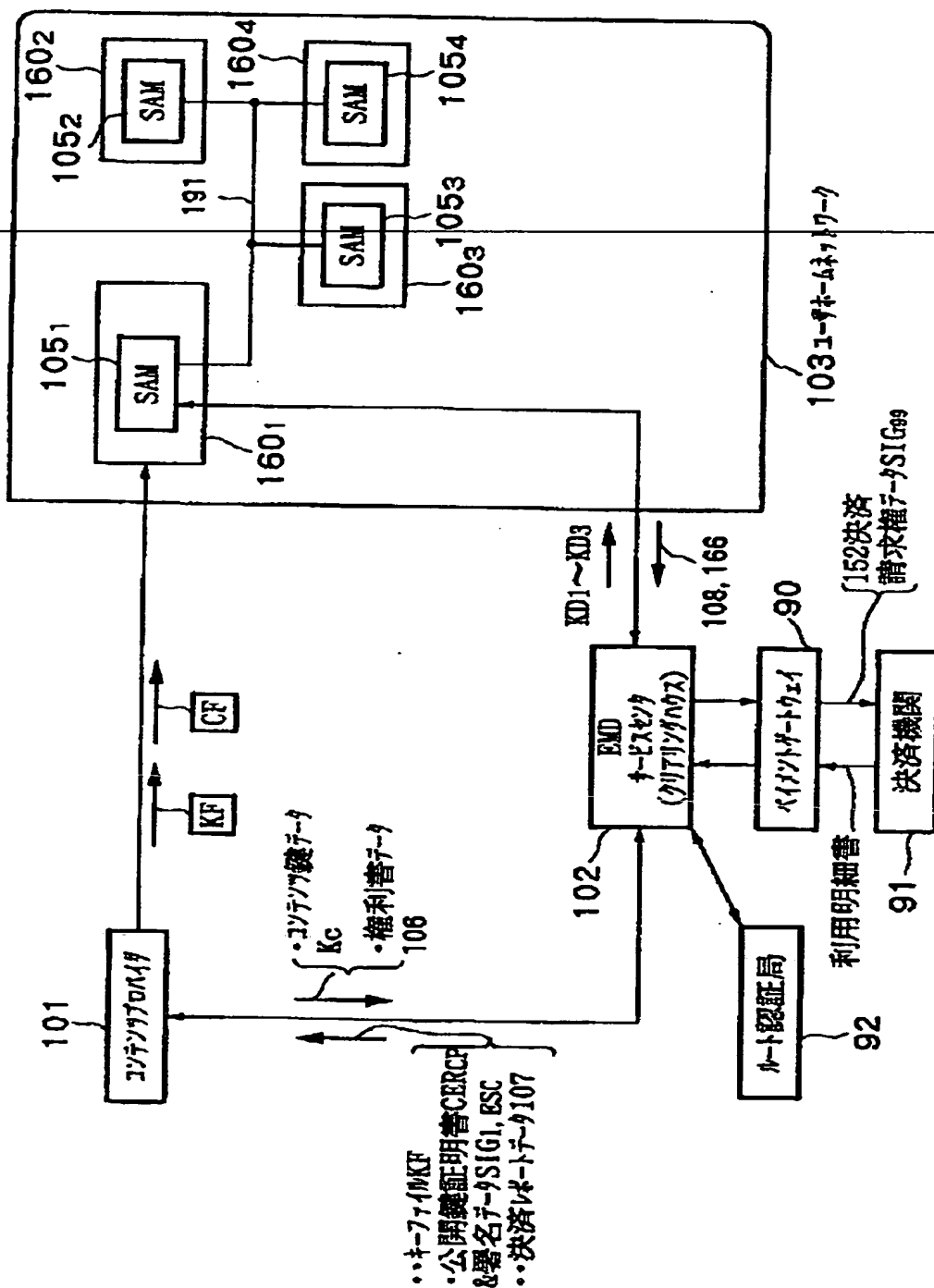
【図 49】



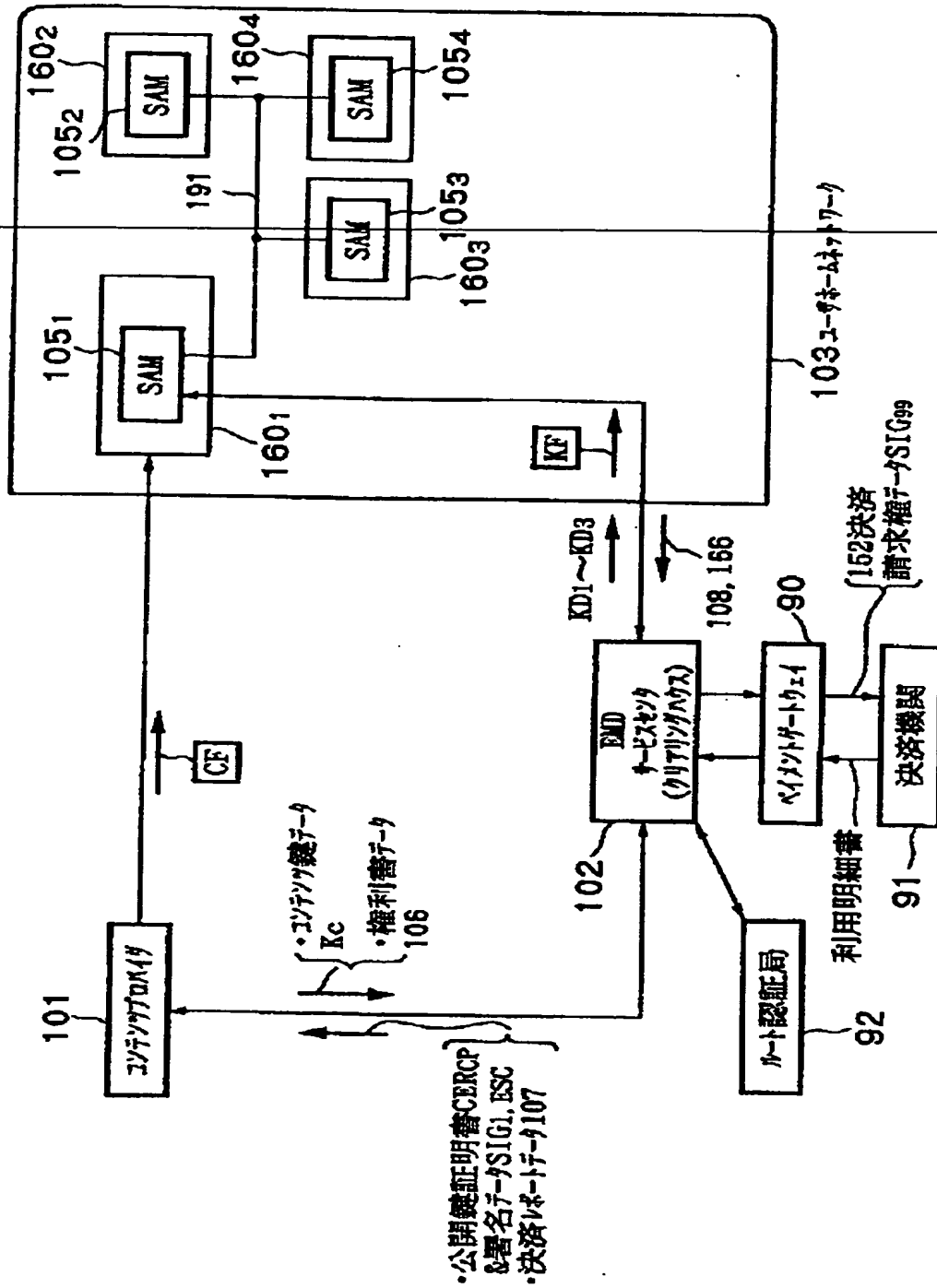
【図 50】



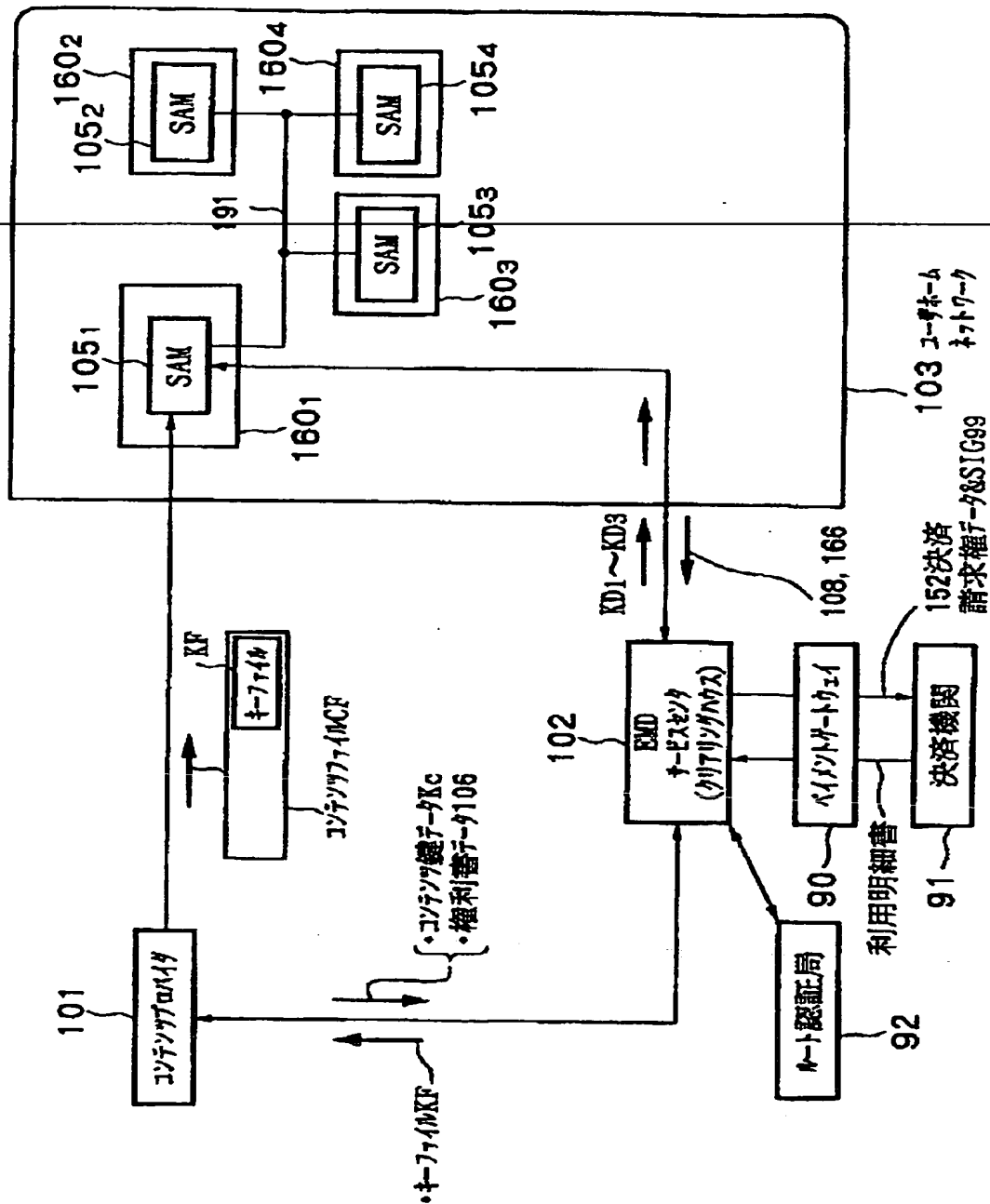
【図 5 1】



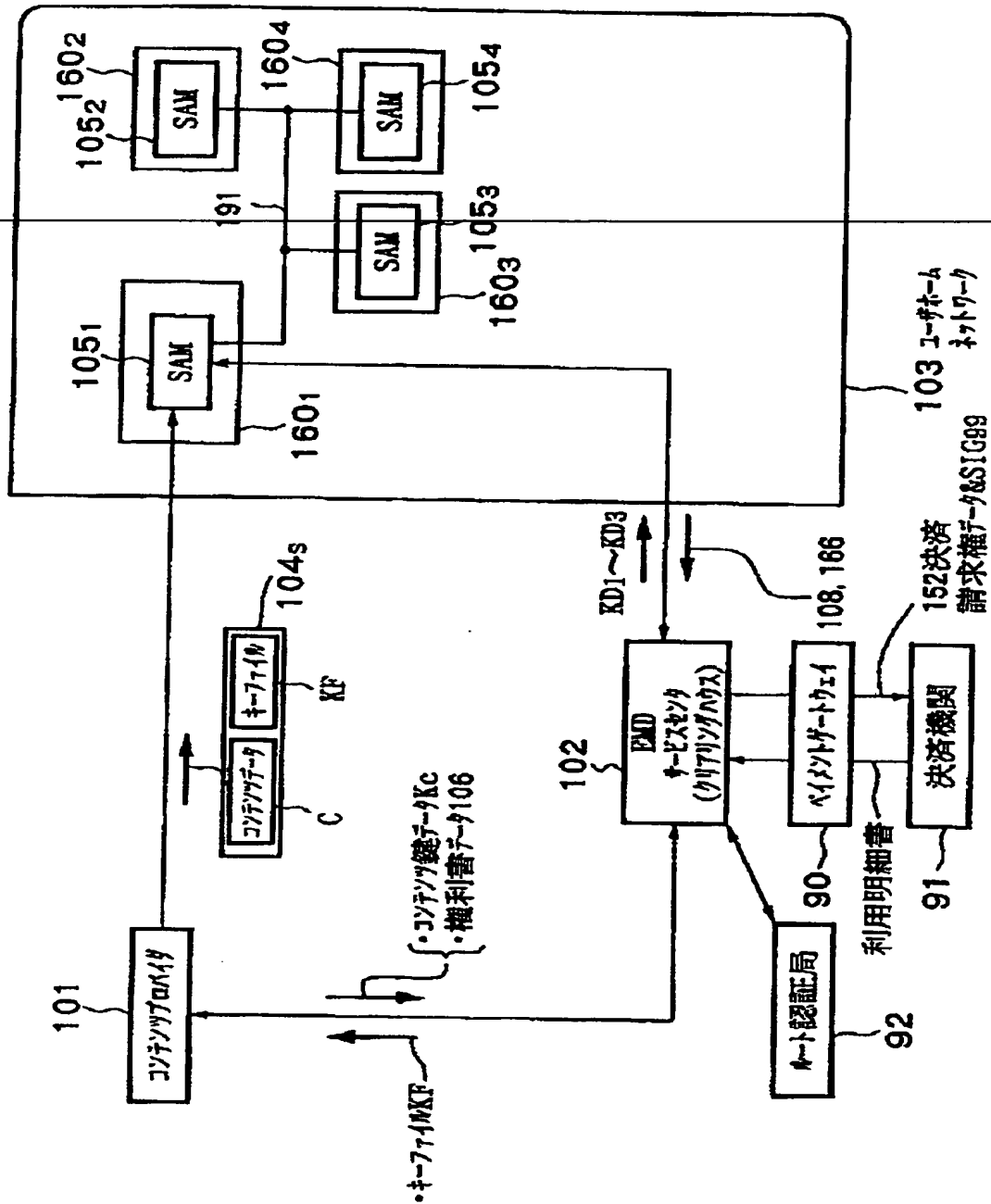
【図 5 2】



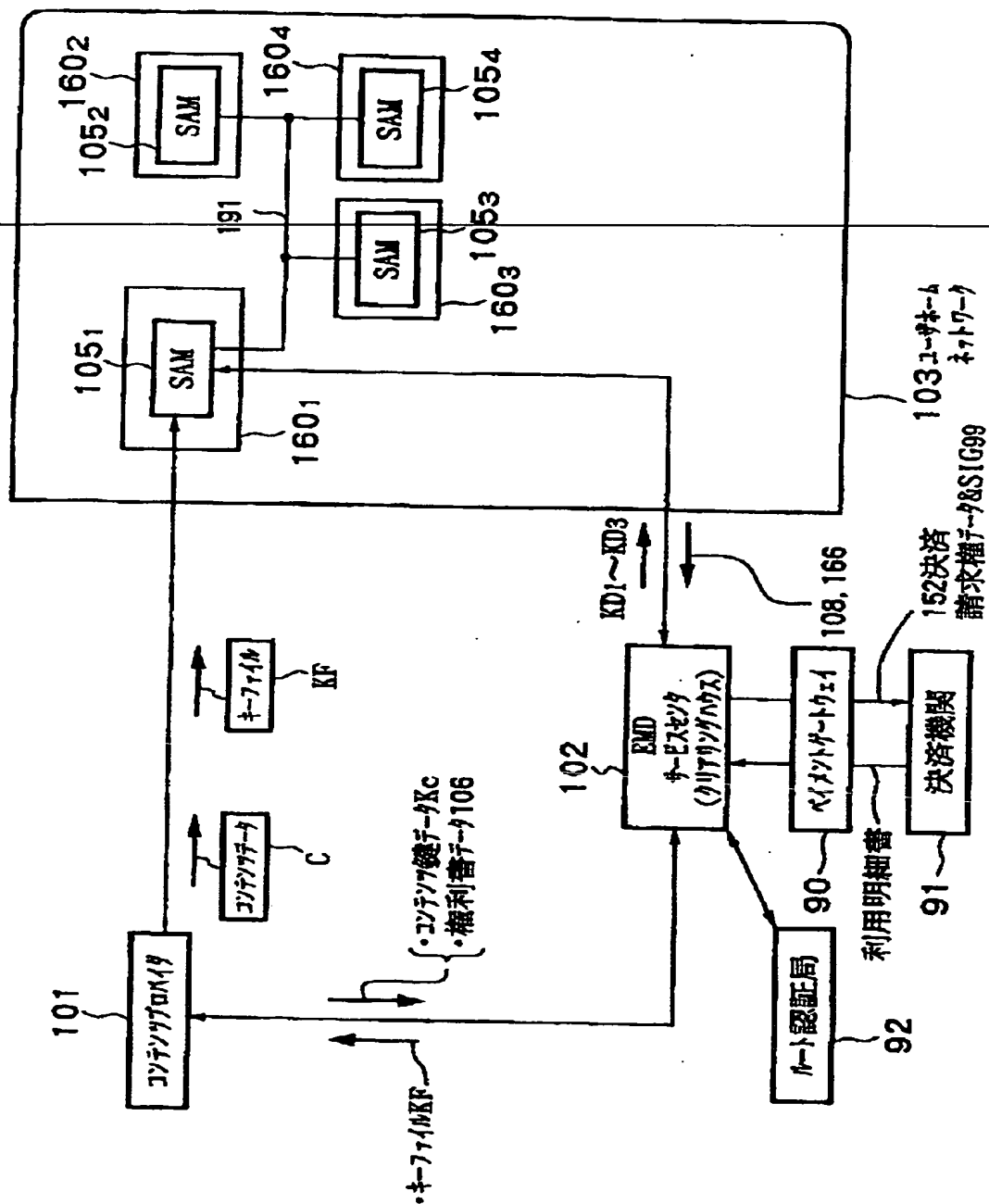
【图 5 3】



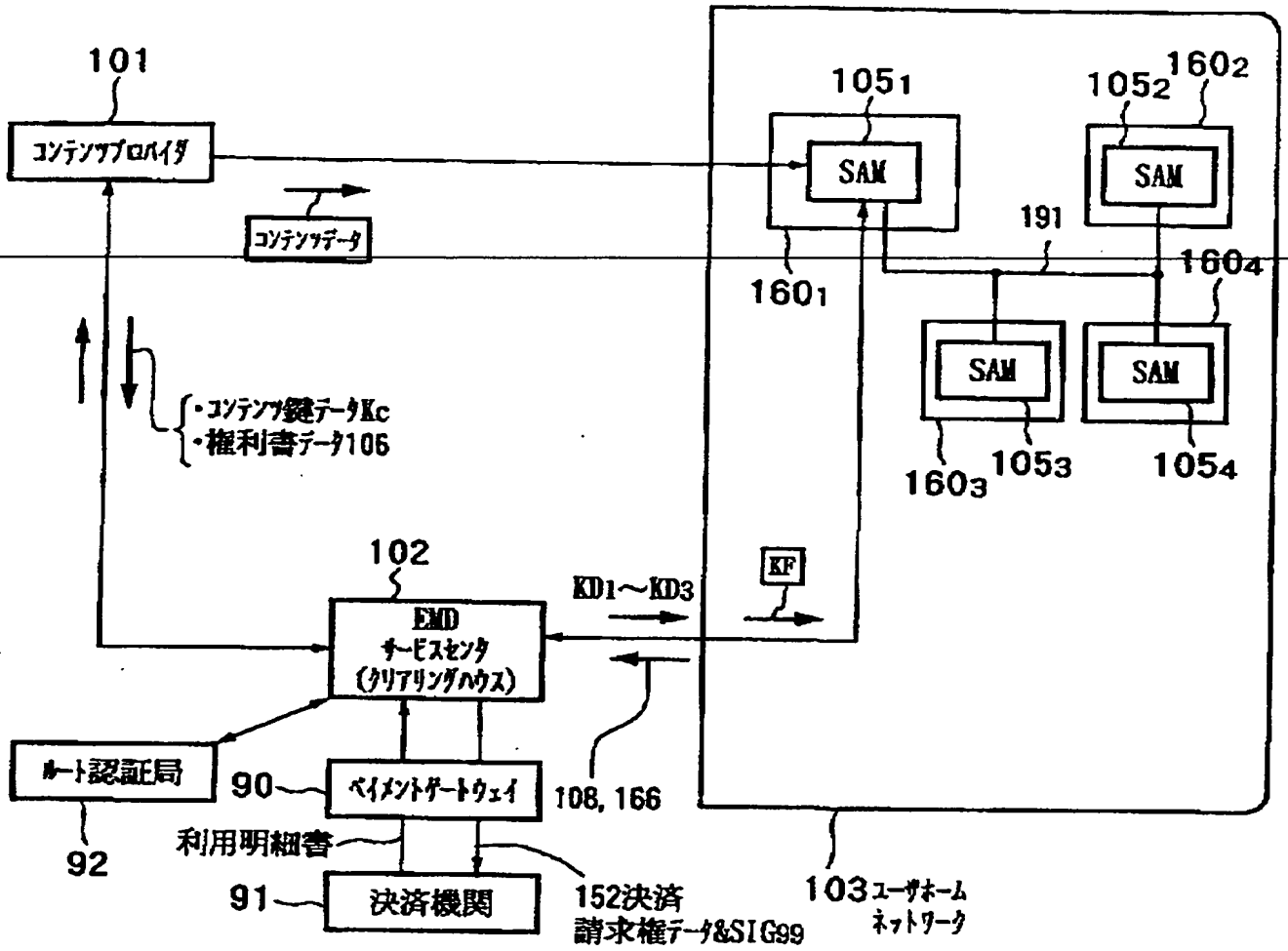
【図 54】



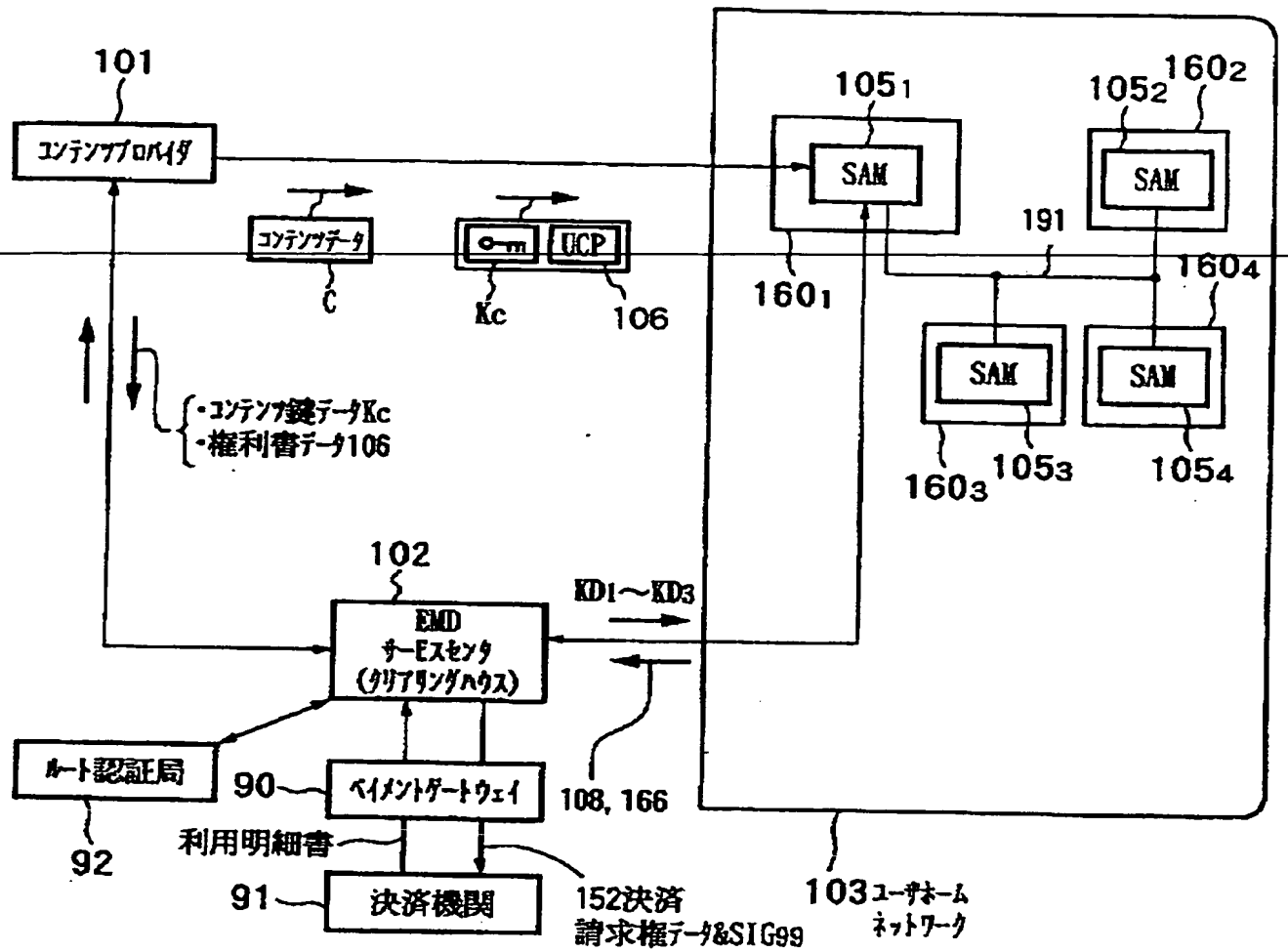
【图 5 5】



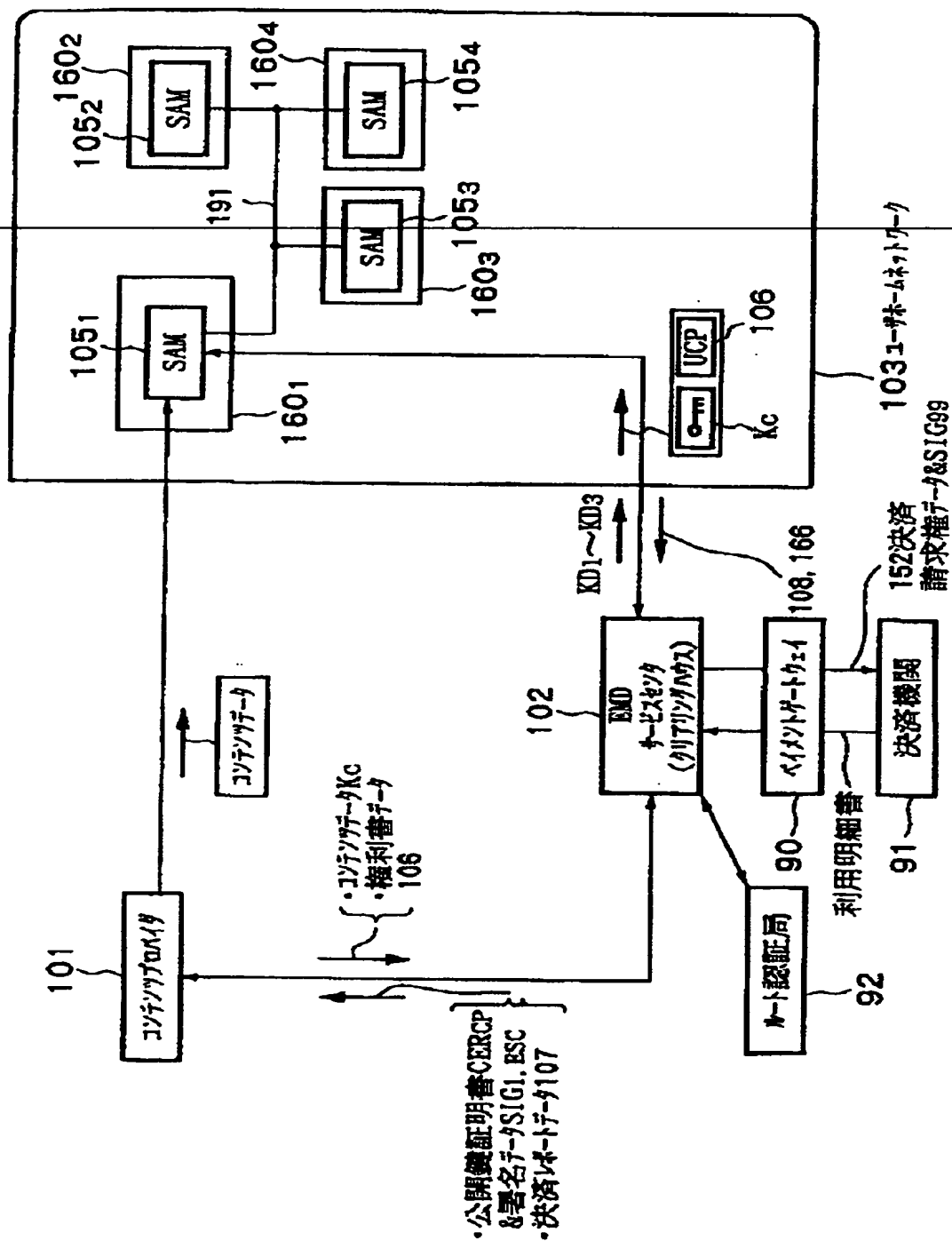
【図 5 6】



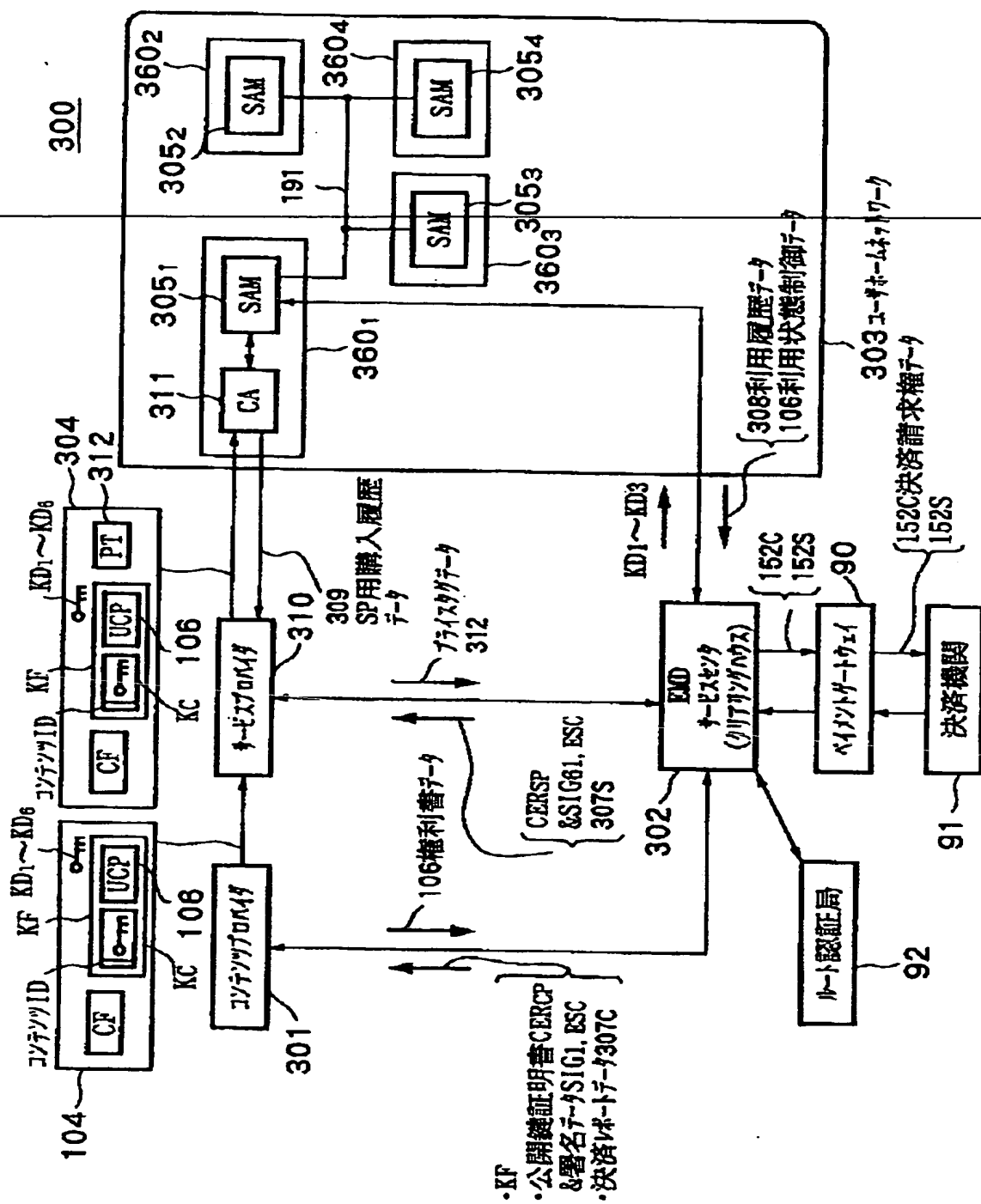
【図 57】



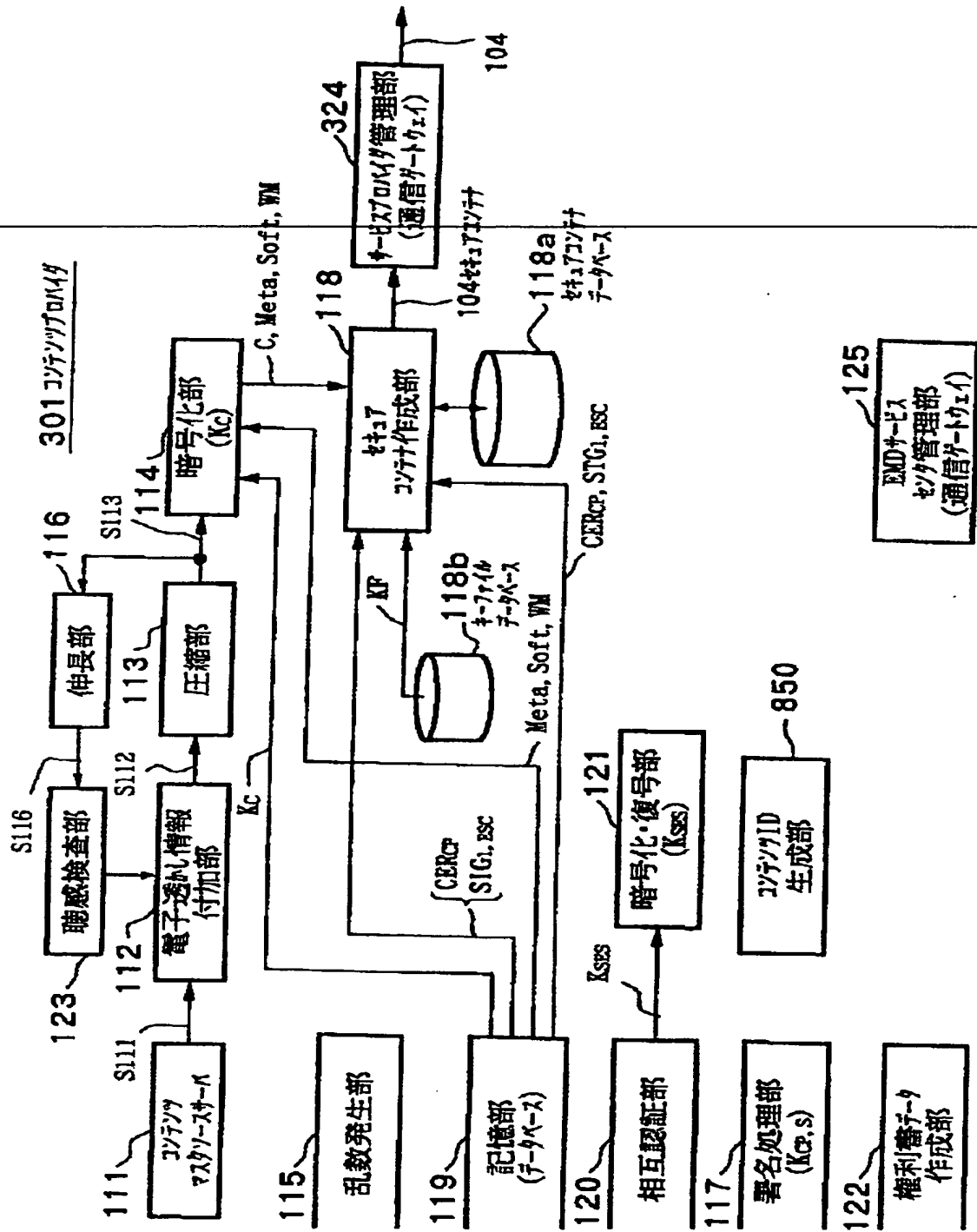
【图 5 8】



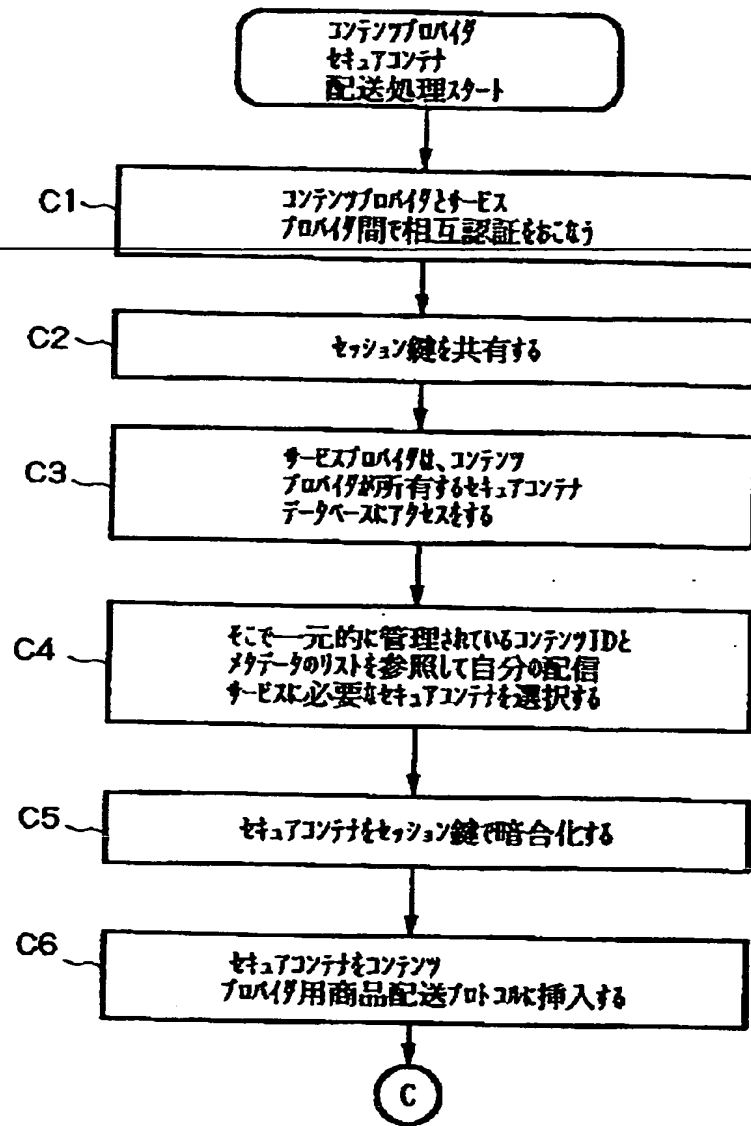
【图 5 9】



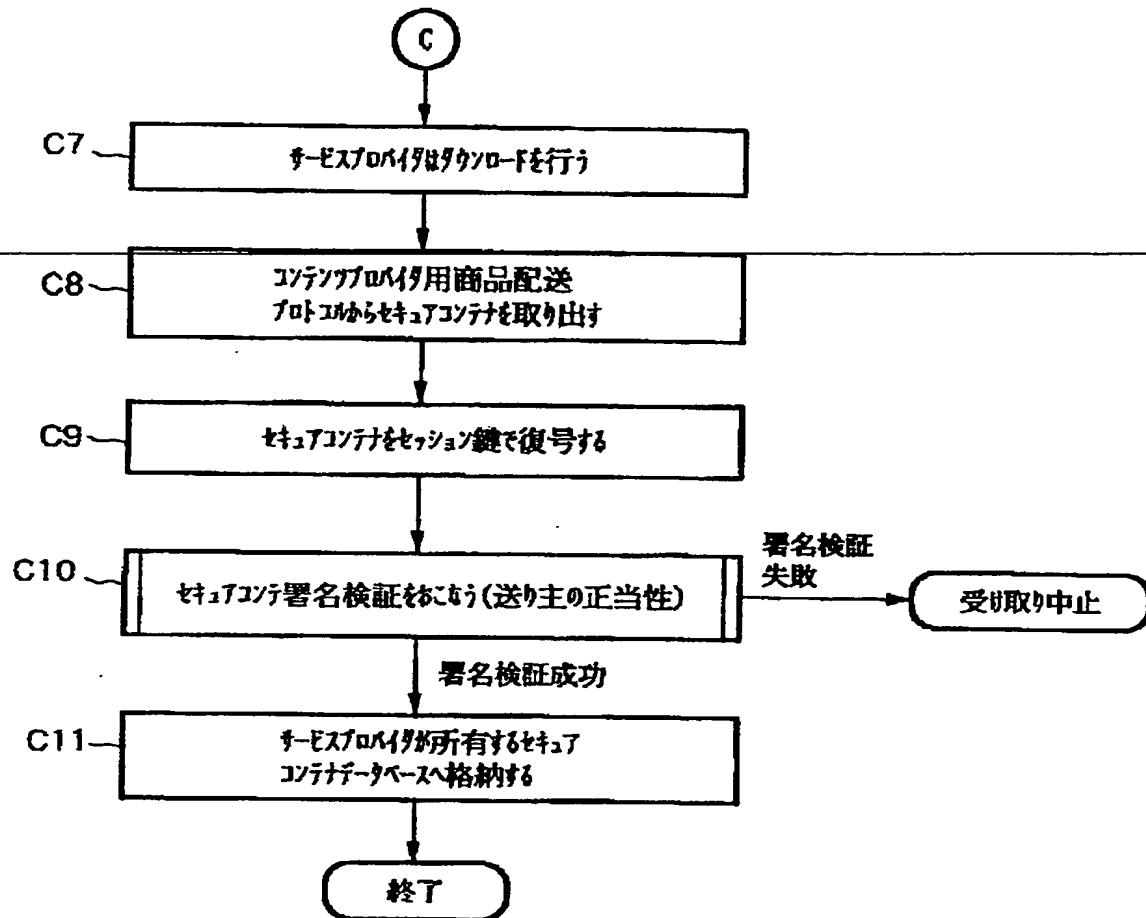
【図 6 0】



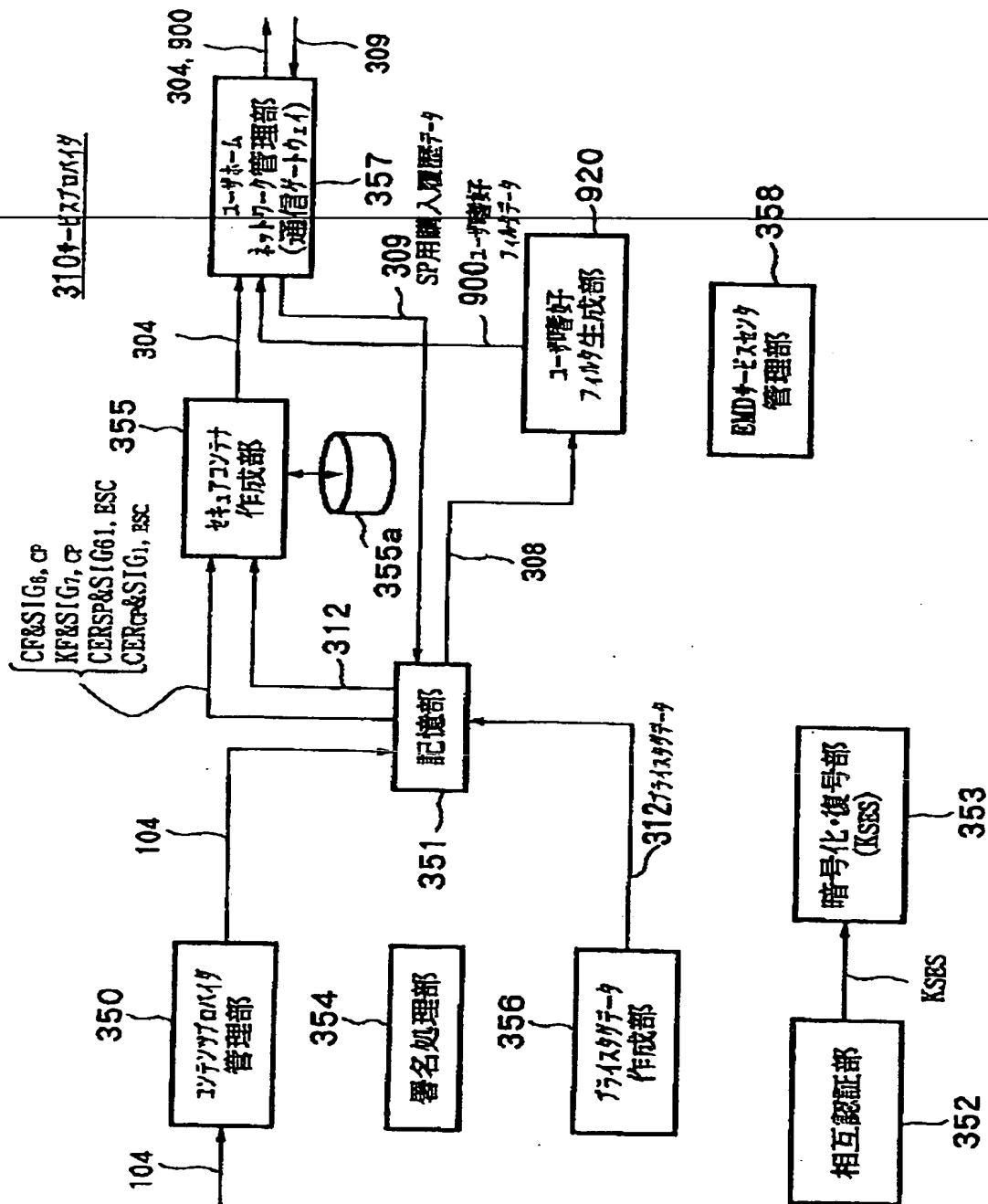
【図 6 1】



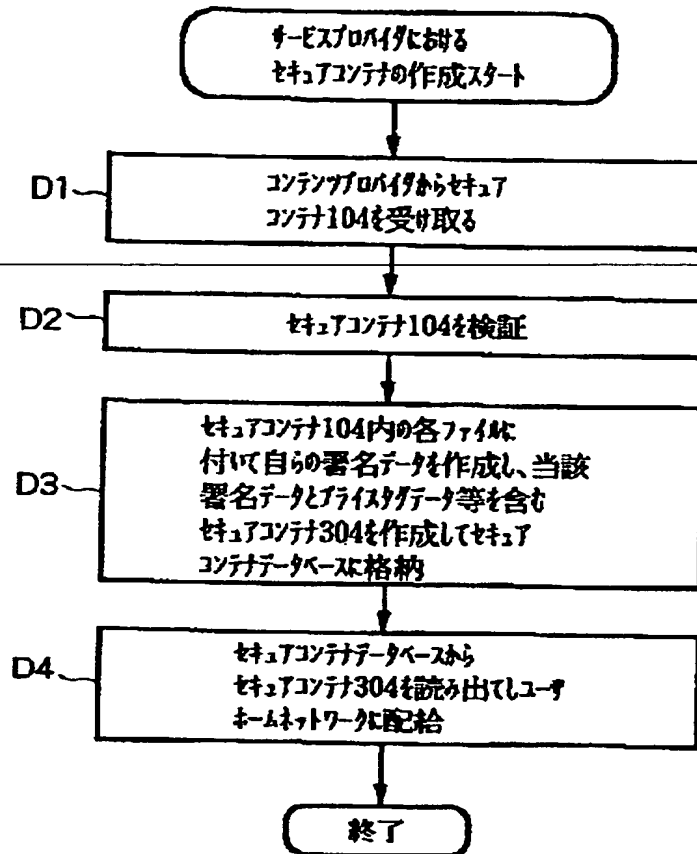
【図 6 2】



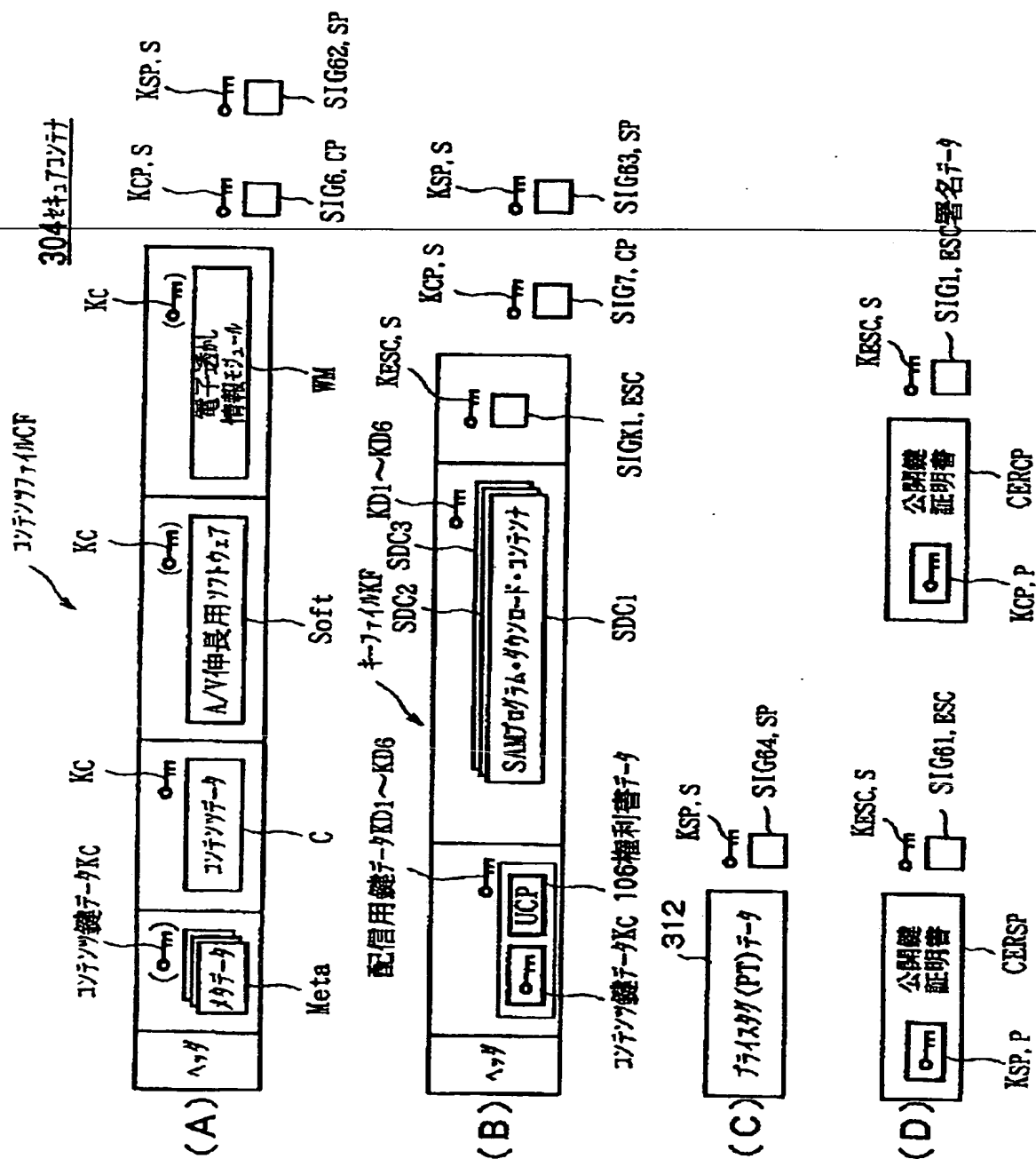
【図 63】



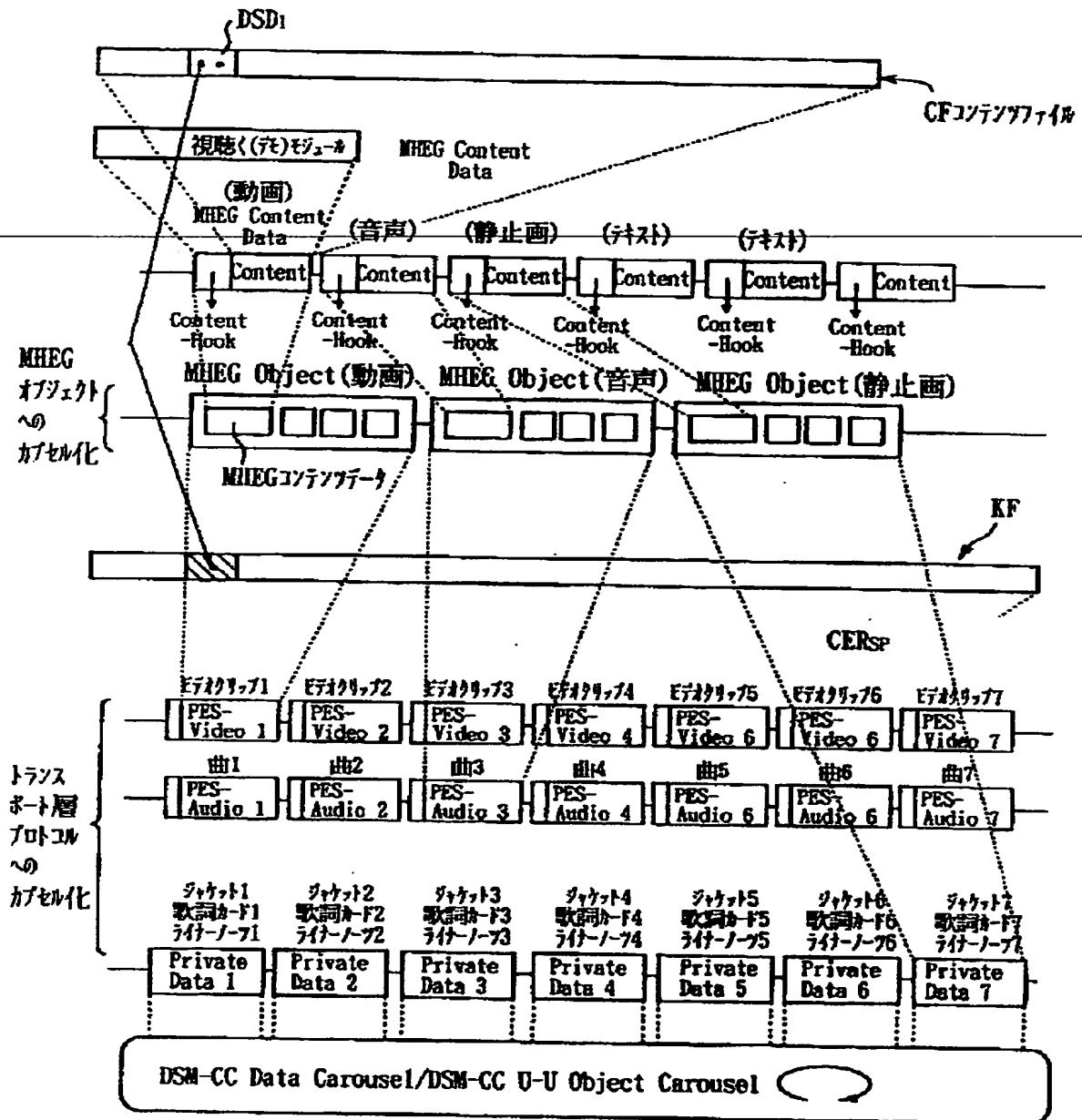
【図 6 4】



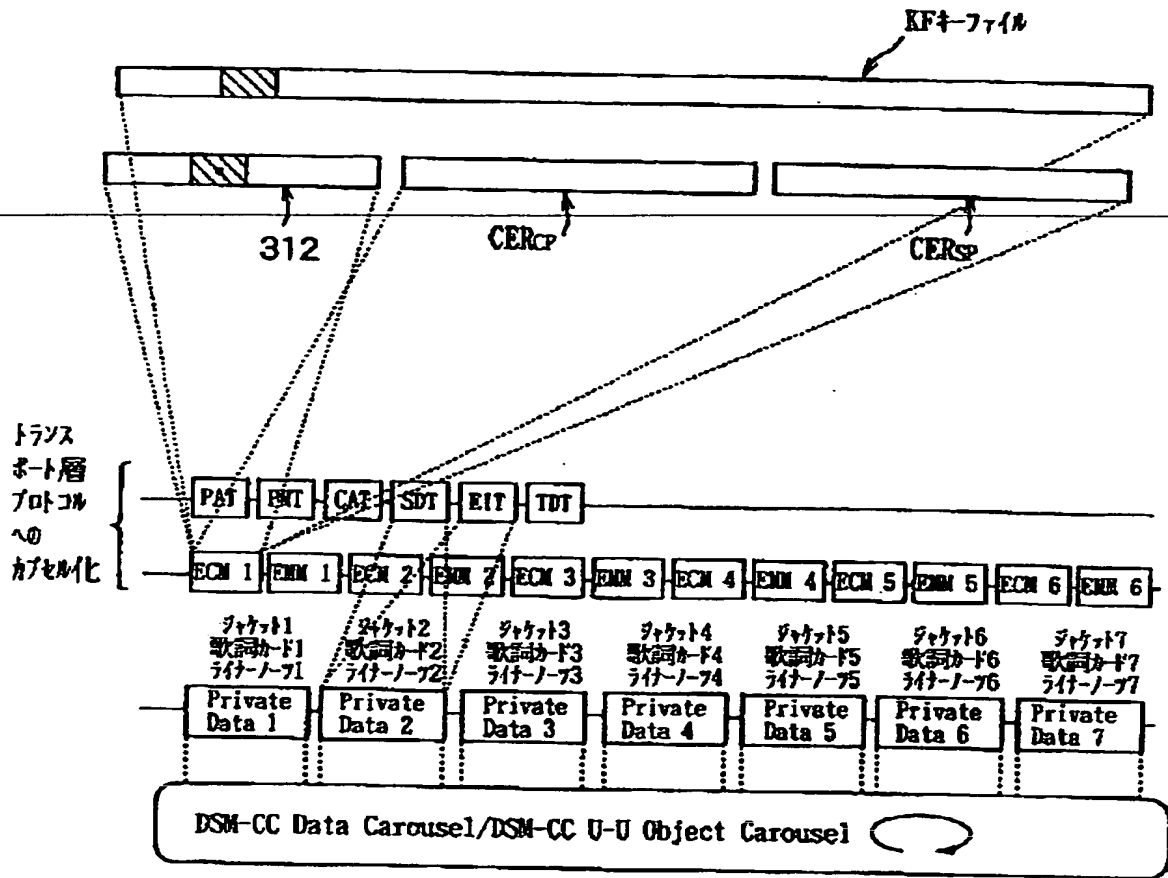
【図 6 5】



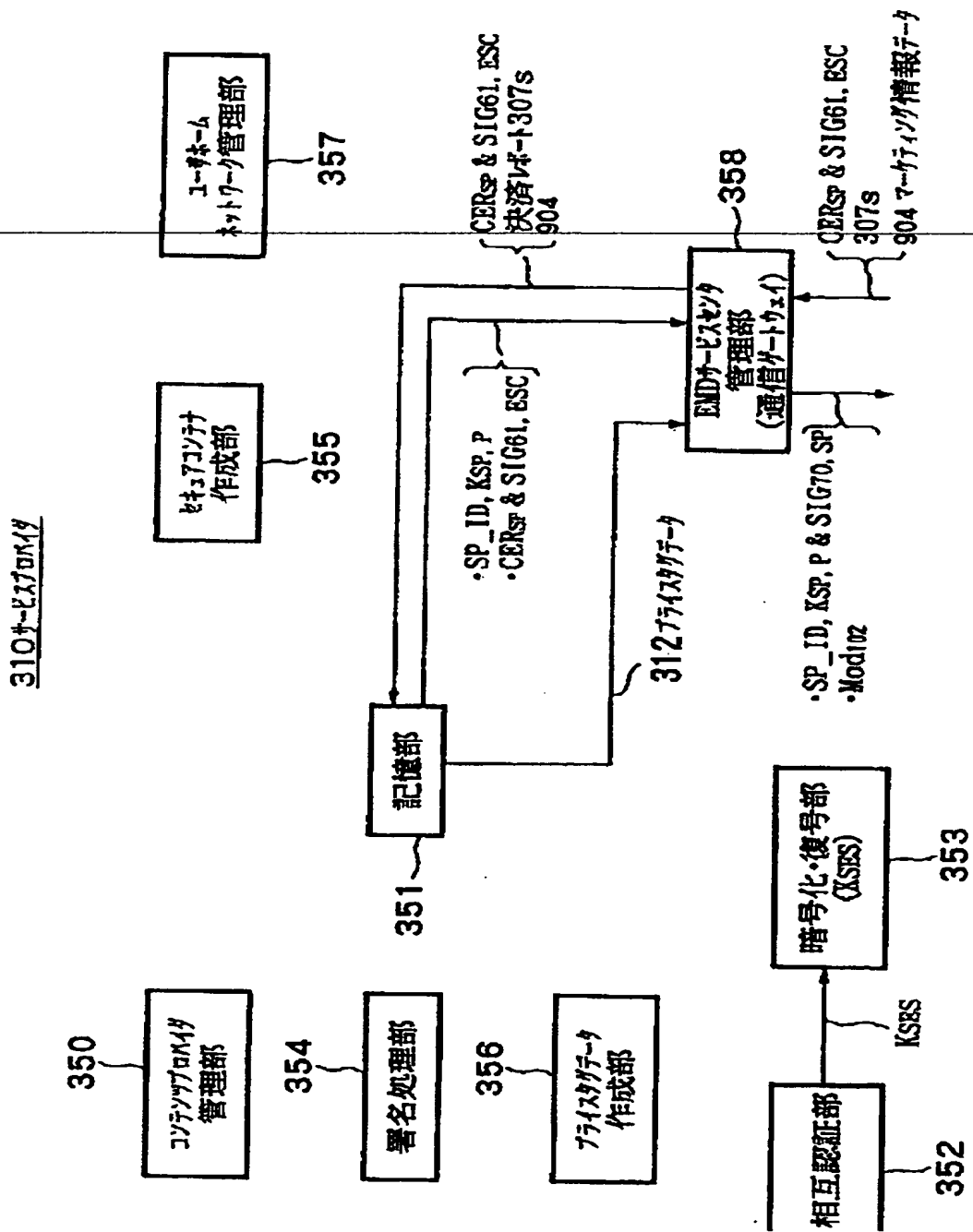
【図 66】



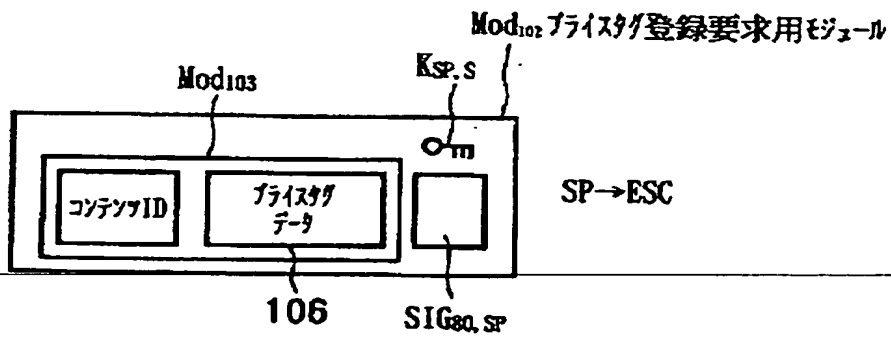
【図 67】



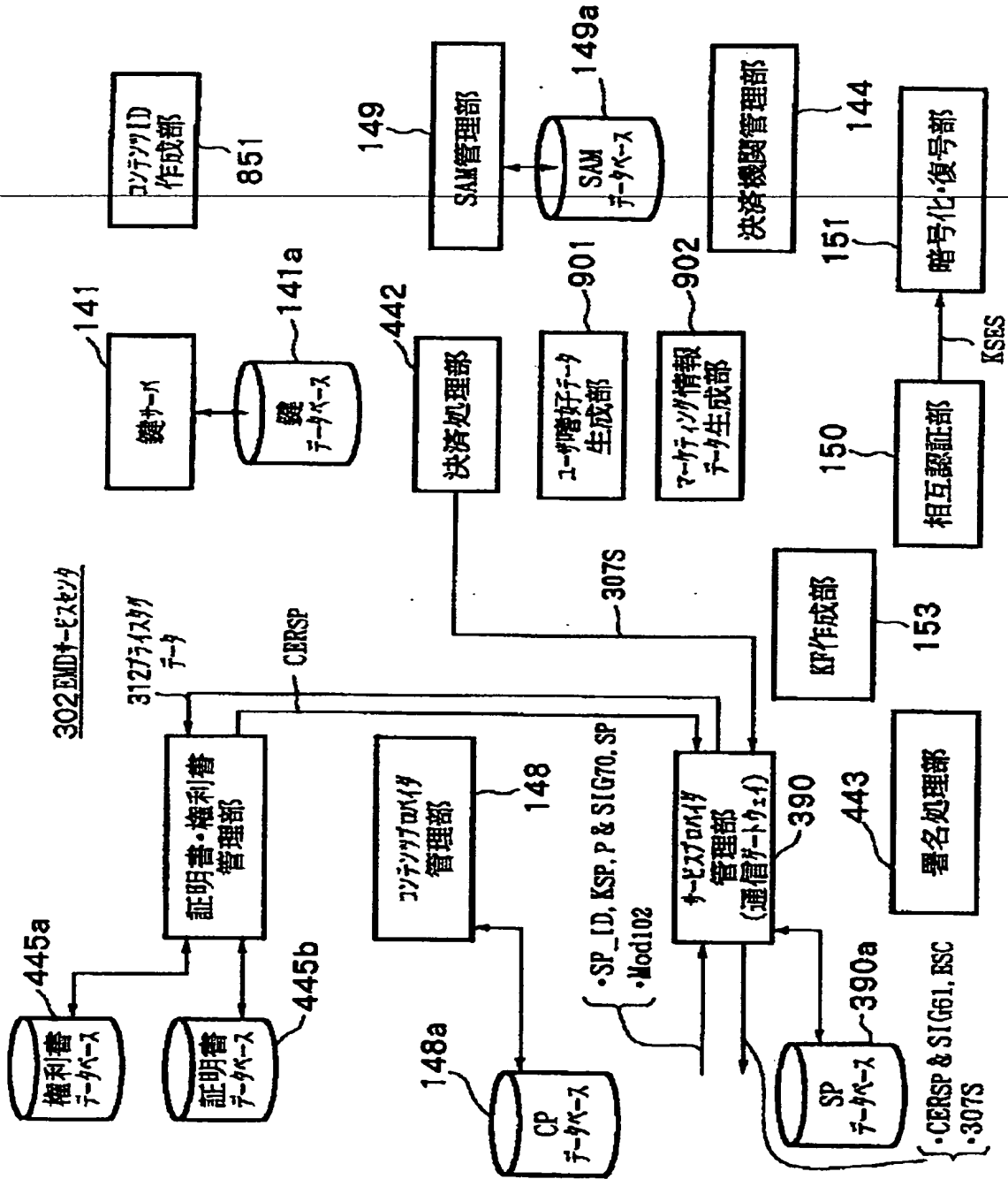
【図 68】



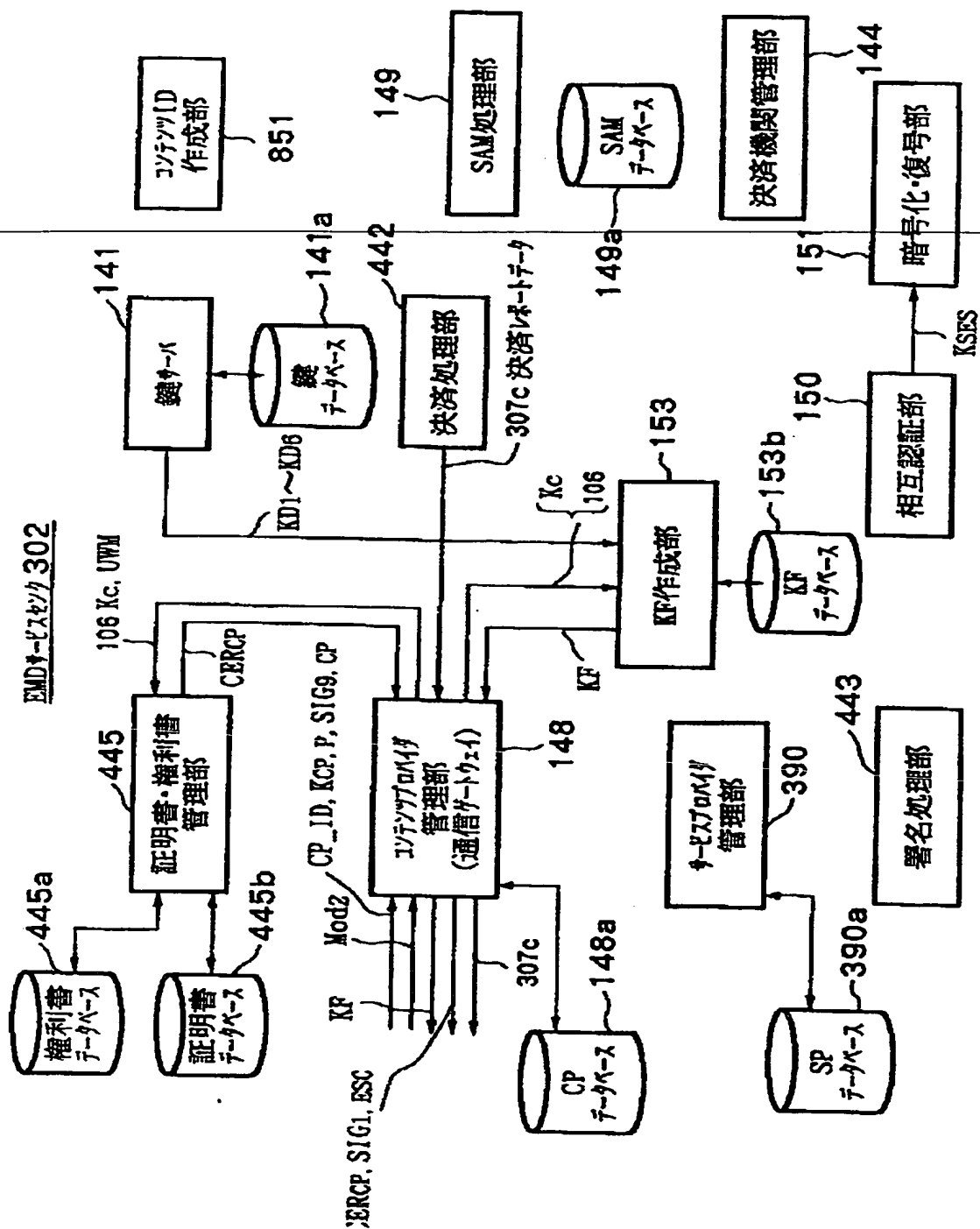
【図 6 9】



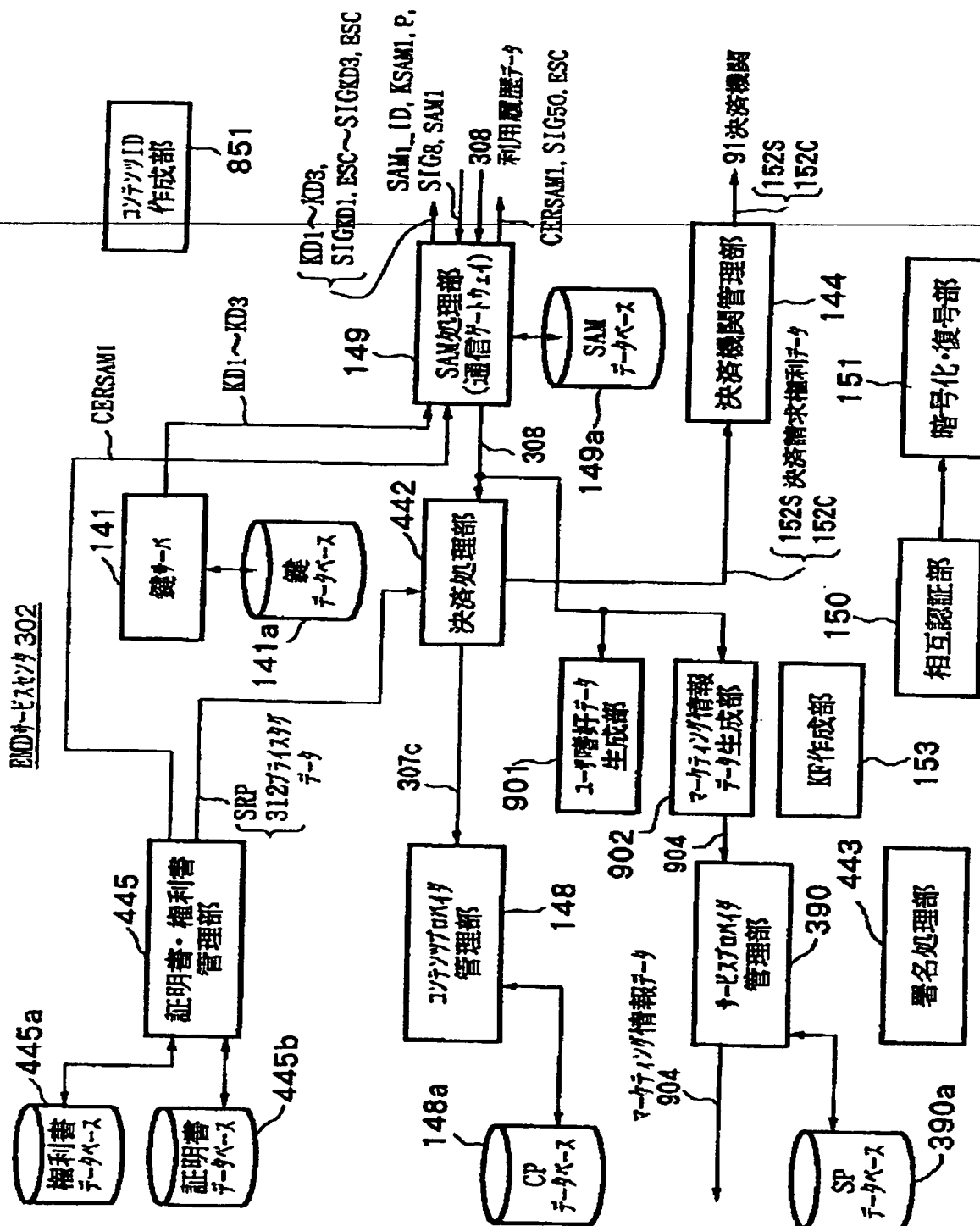
【図 7 0】



【图 7 1】



【图 7 2】



【図 7 3】

利用履歴データ308の内容

識別子Content_ID

識別子CP_ID

識別子SP_ID

コンテンツデータの信号諸元データ

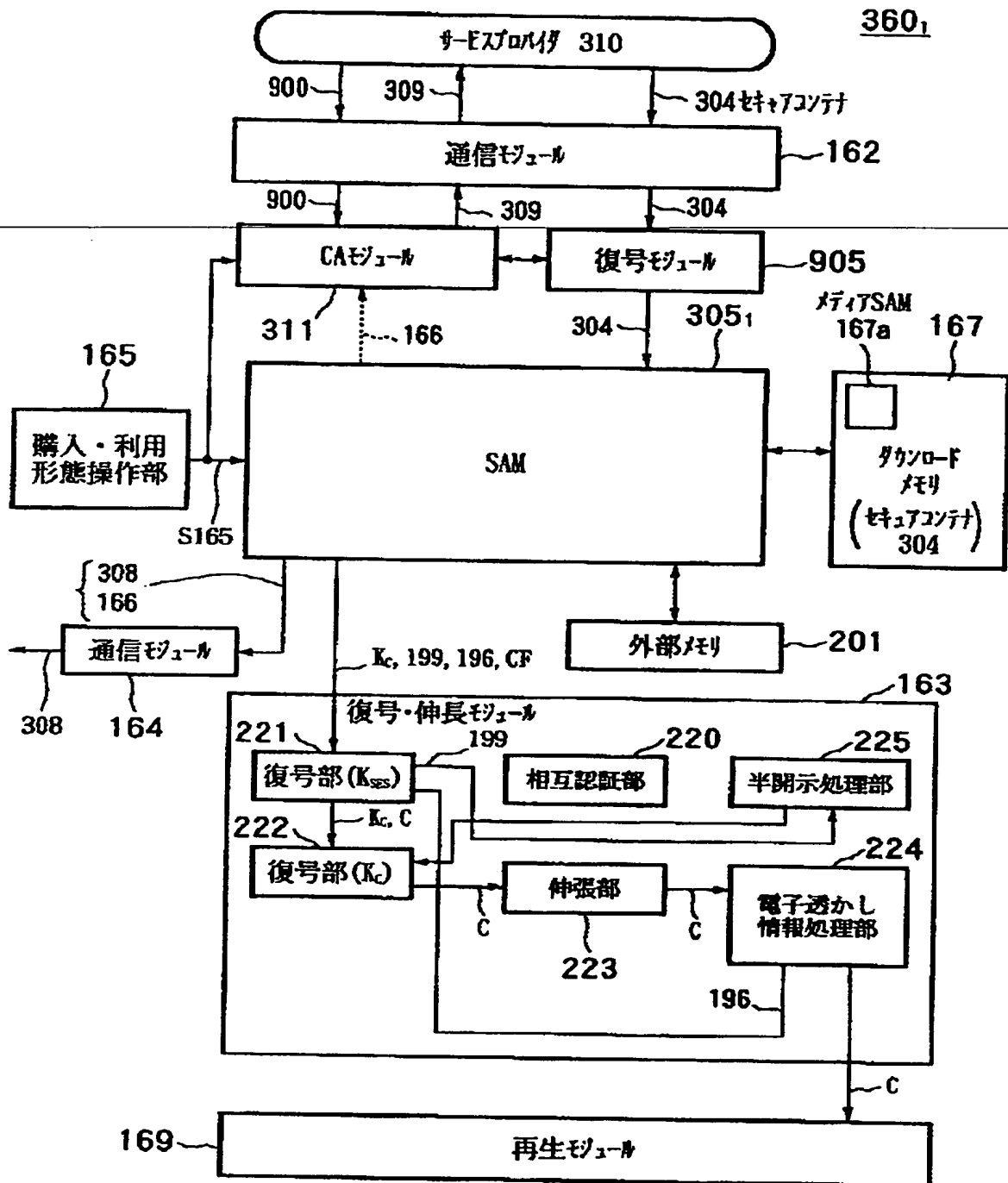
コンテンツデータの圧縮方法

記録媒体の識別子Media_ID

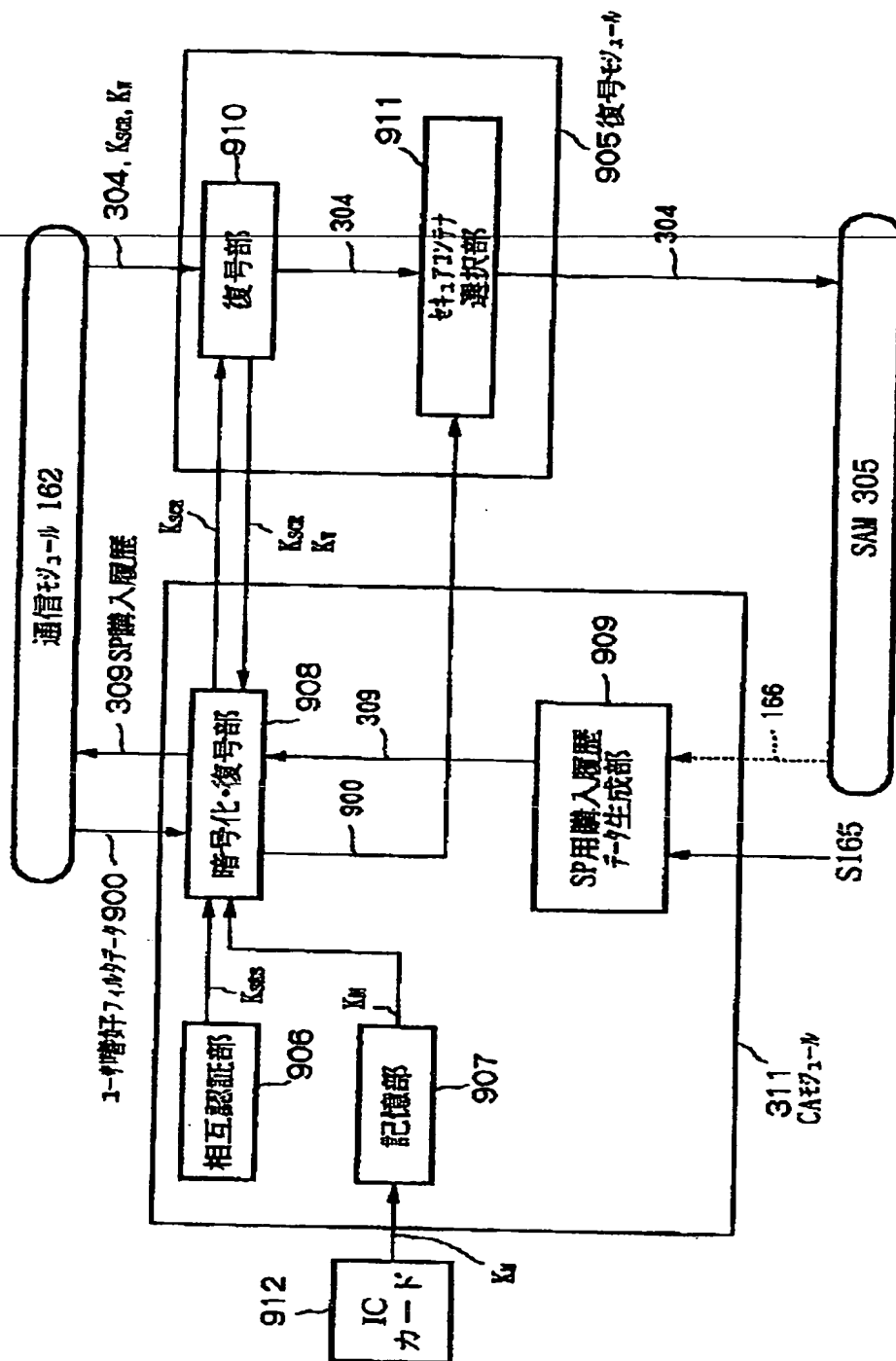
識別子SAM_ID、

ユーザのUSER_ID

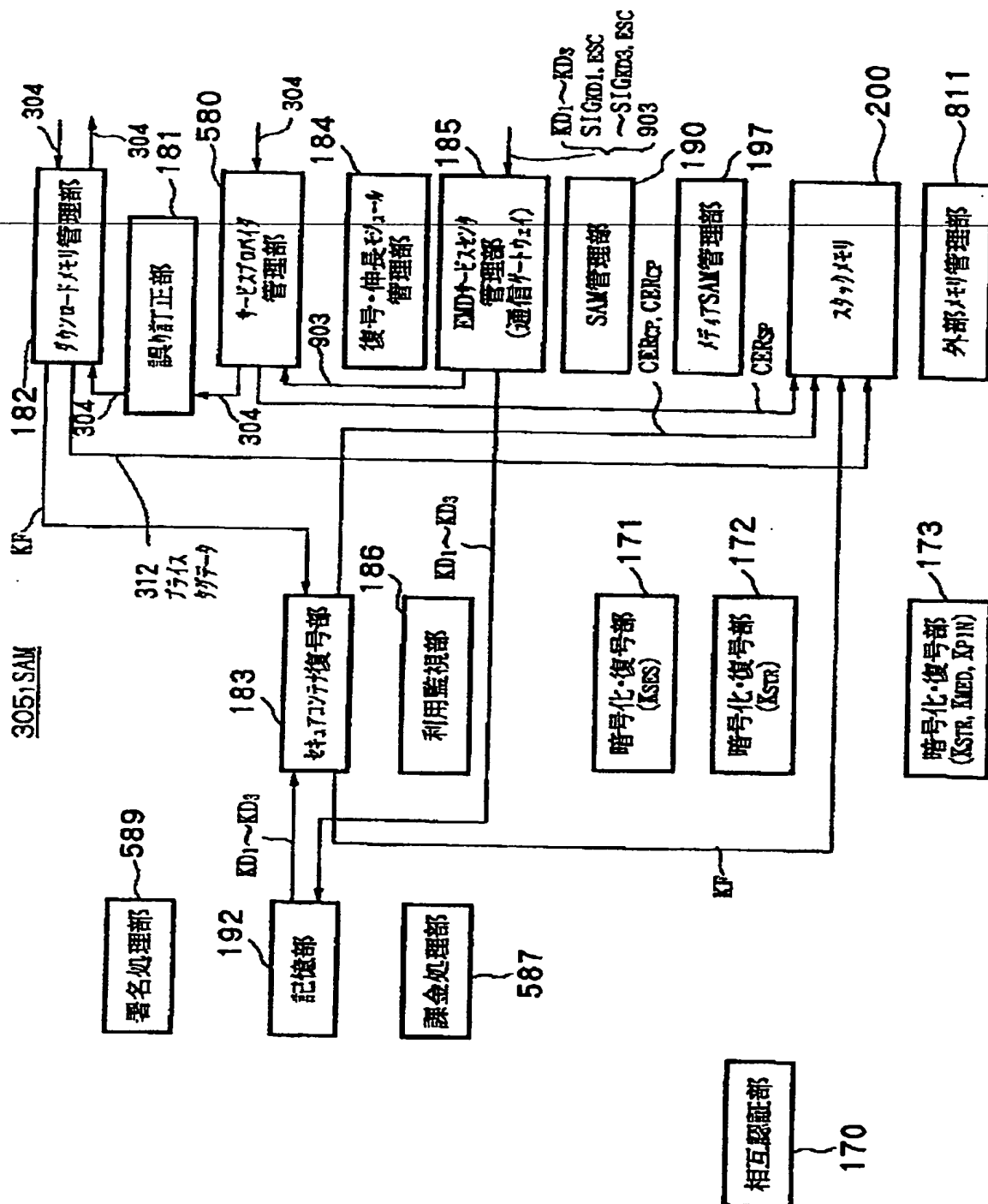
【図 74】



【図 7 5】



【図 76】



【図 7 7】

スタックメモリ200の記憶データ

コンテンツ鍵データK_C

権利書データ(UCP) 106

不揮発性メモリ201のロック鍵データK_{Loc}

コンテンツプロバイダ301の公開鍵証明書データCER_{CP}

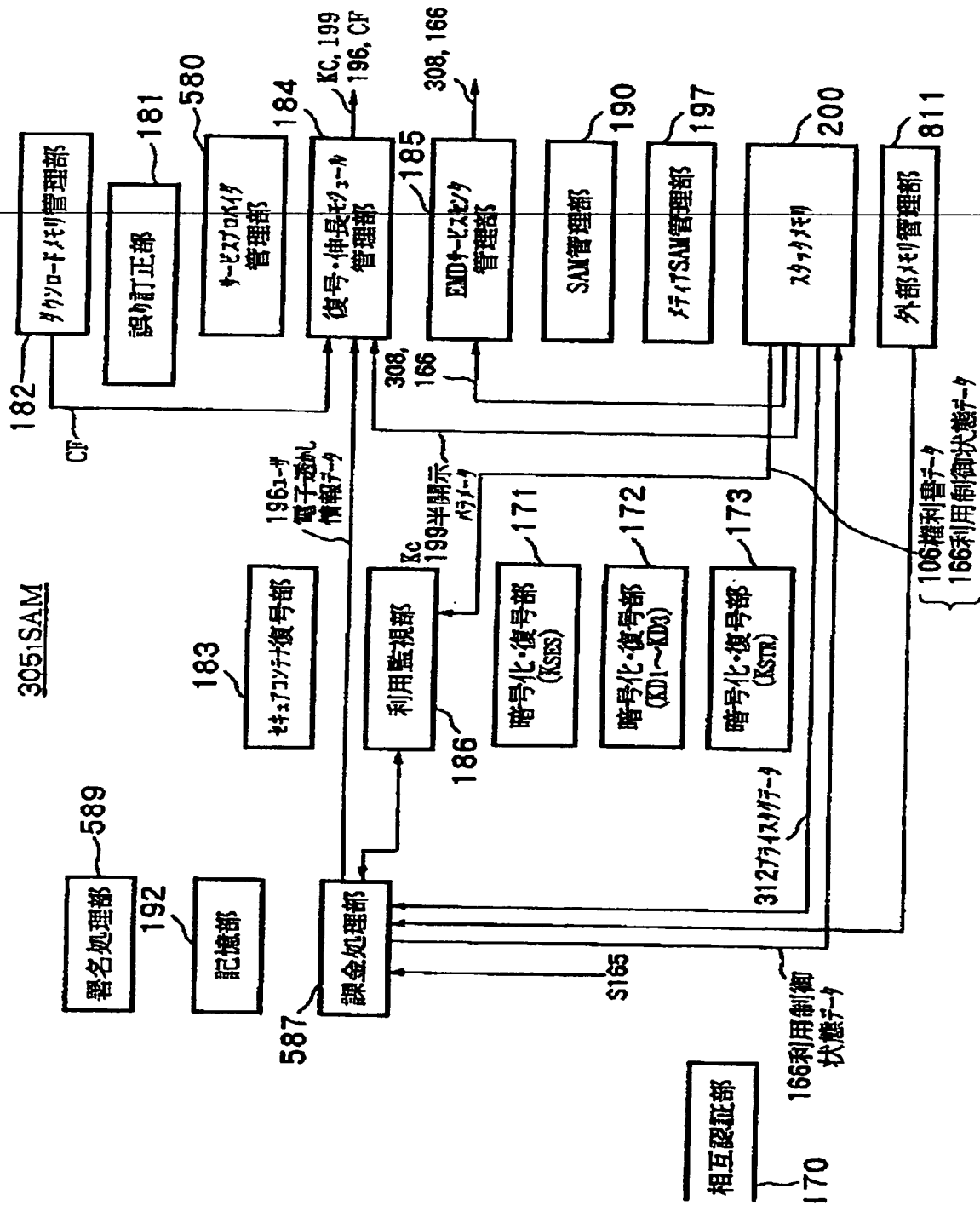
サードプロバイダ301の公開鍵証明書データCER_{SP}

利用制御情状態データ(UCS) 166

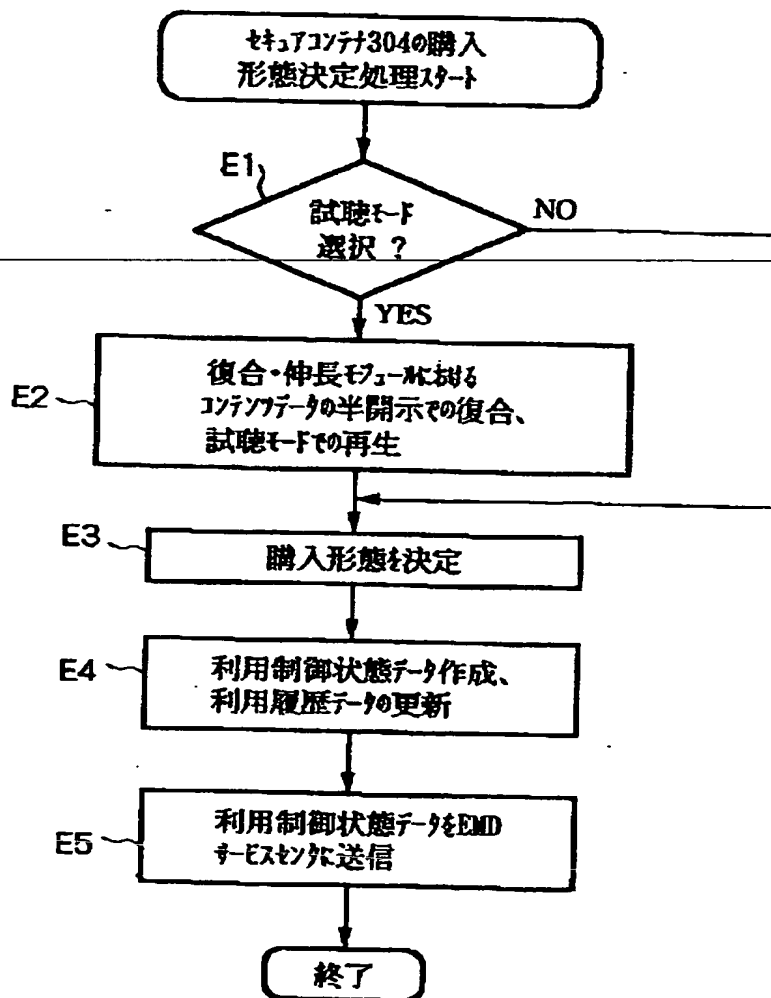
SAMプログラム・ダウンロード・コンテンツSD₁～SD₃

プレイスタグデータ312

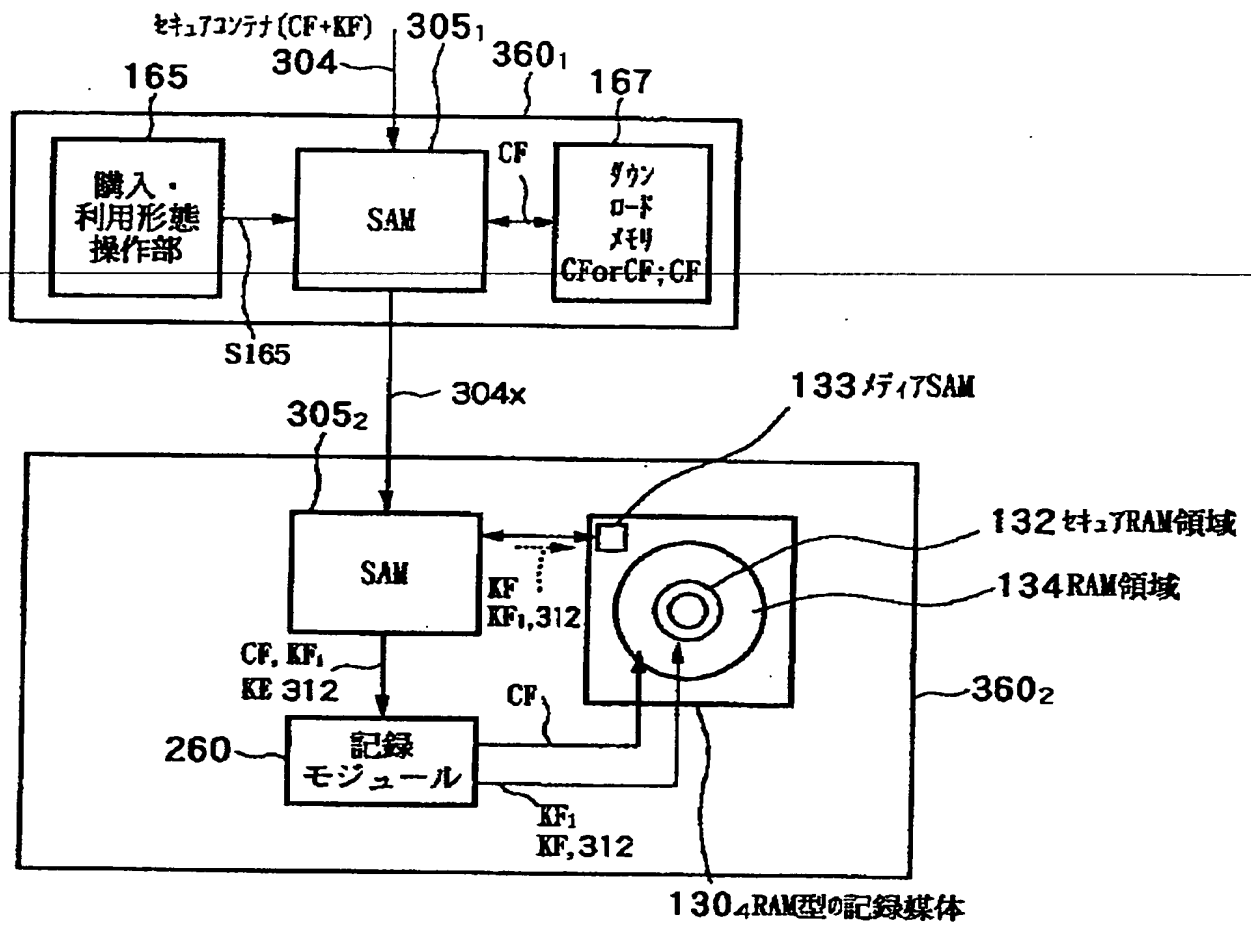
【図 78】



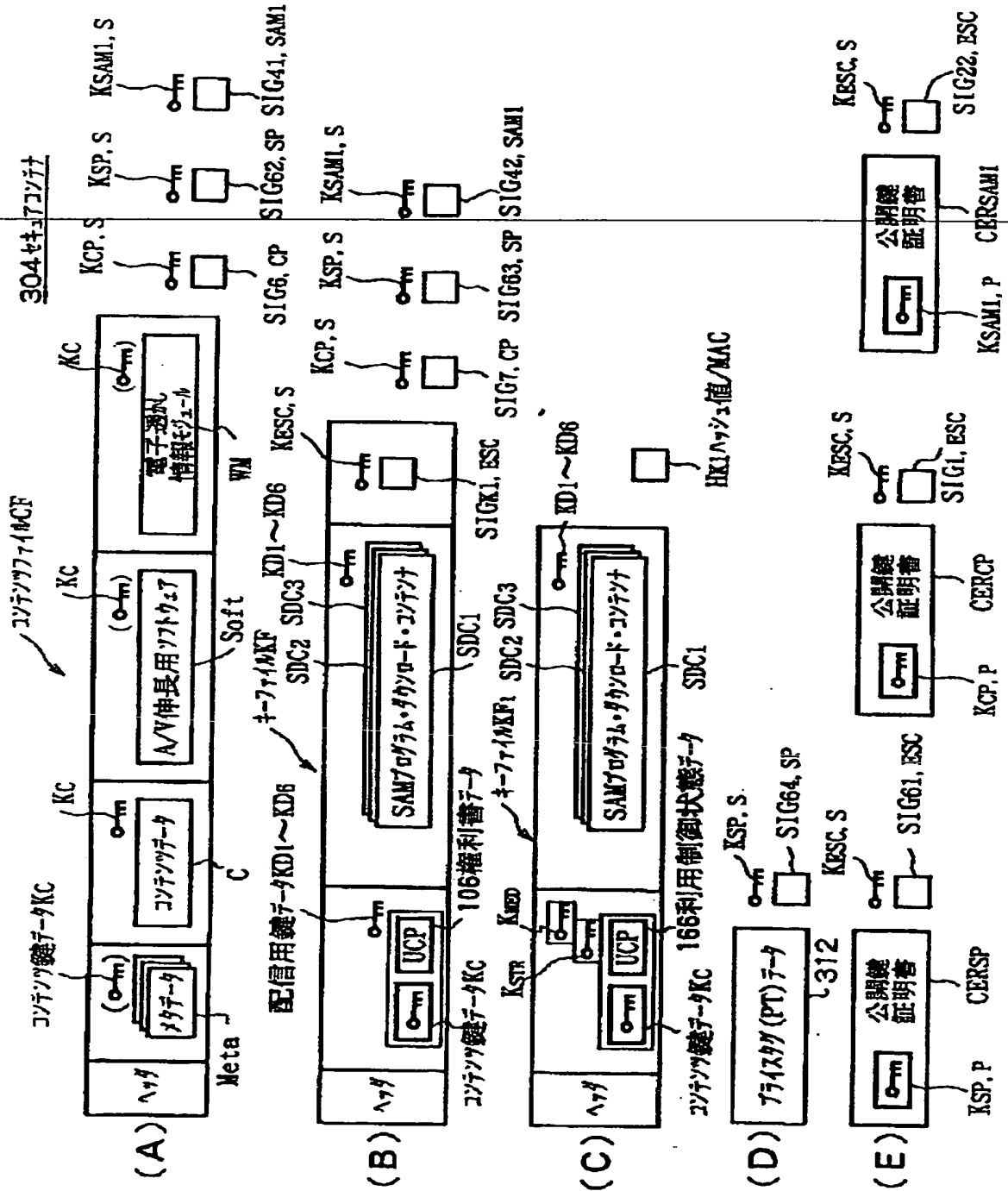
【図 79】



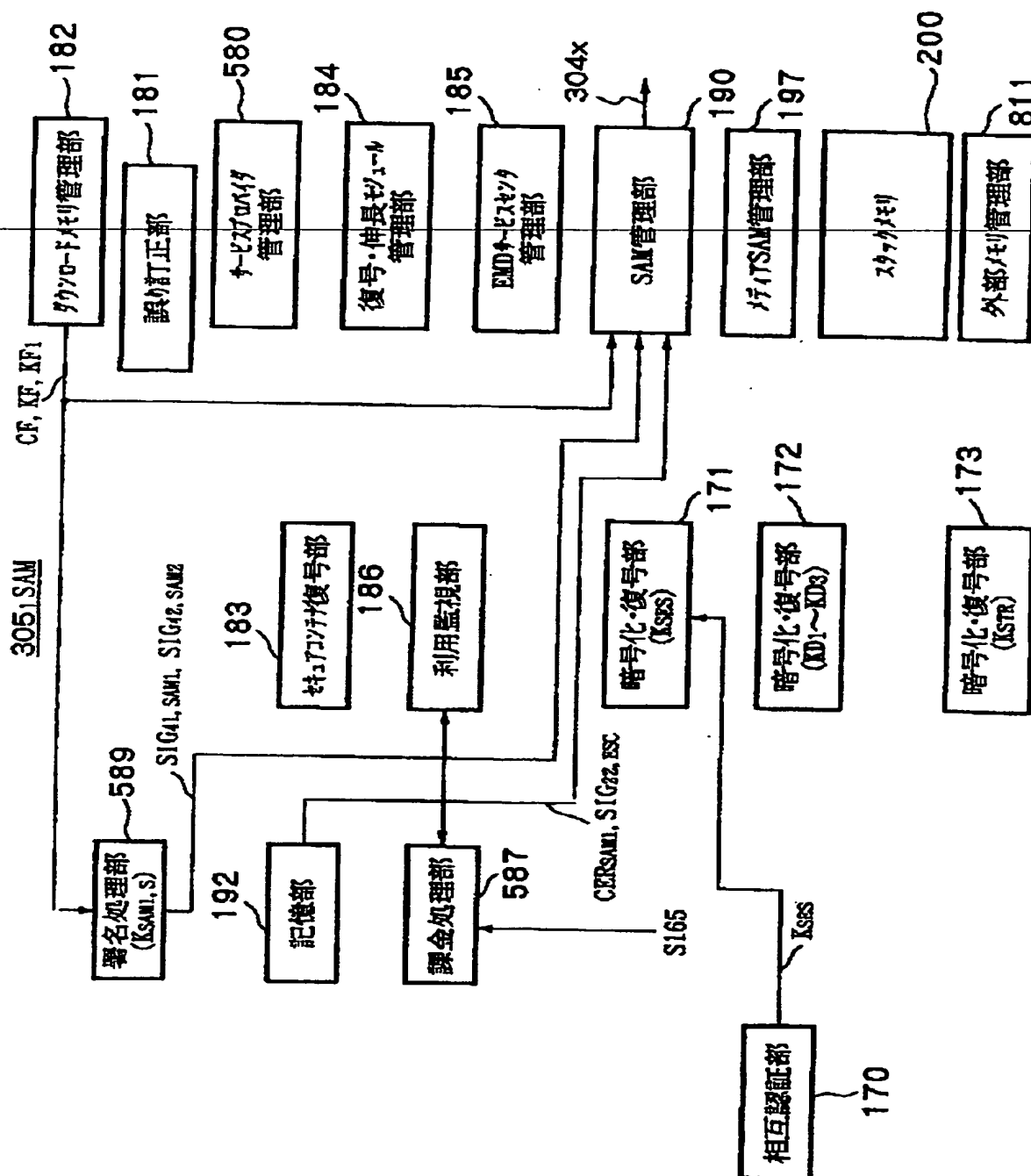
【図 80】



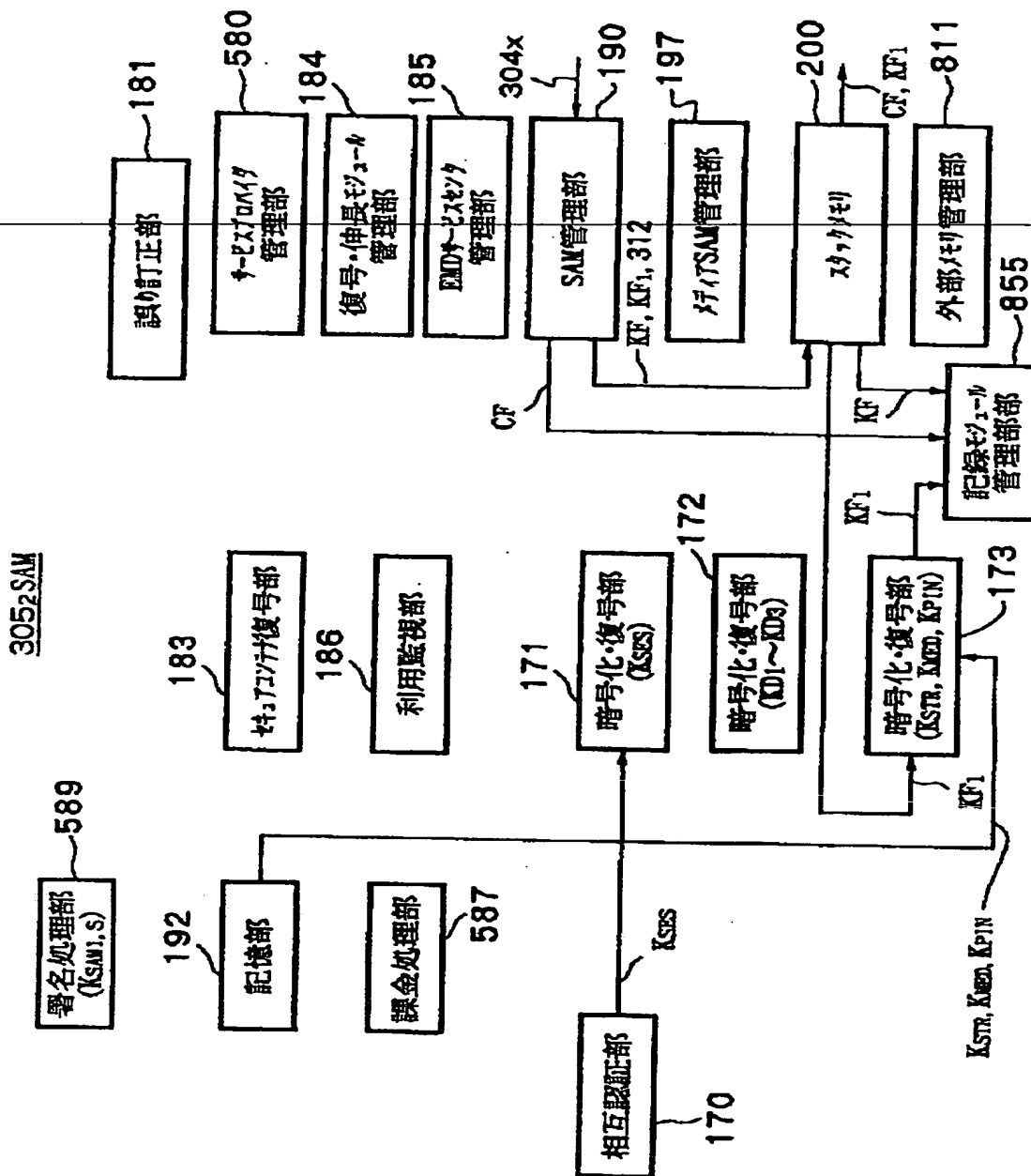
【図 8 1】



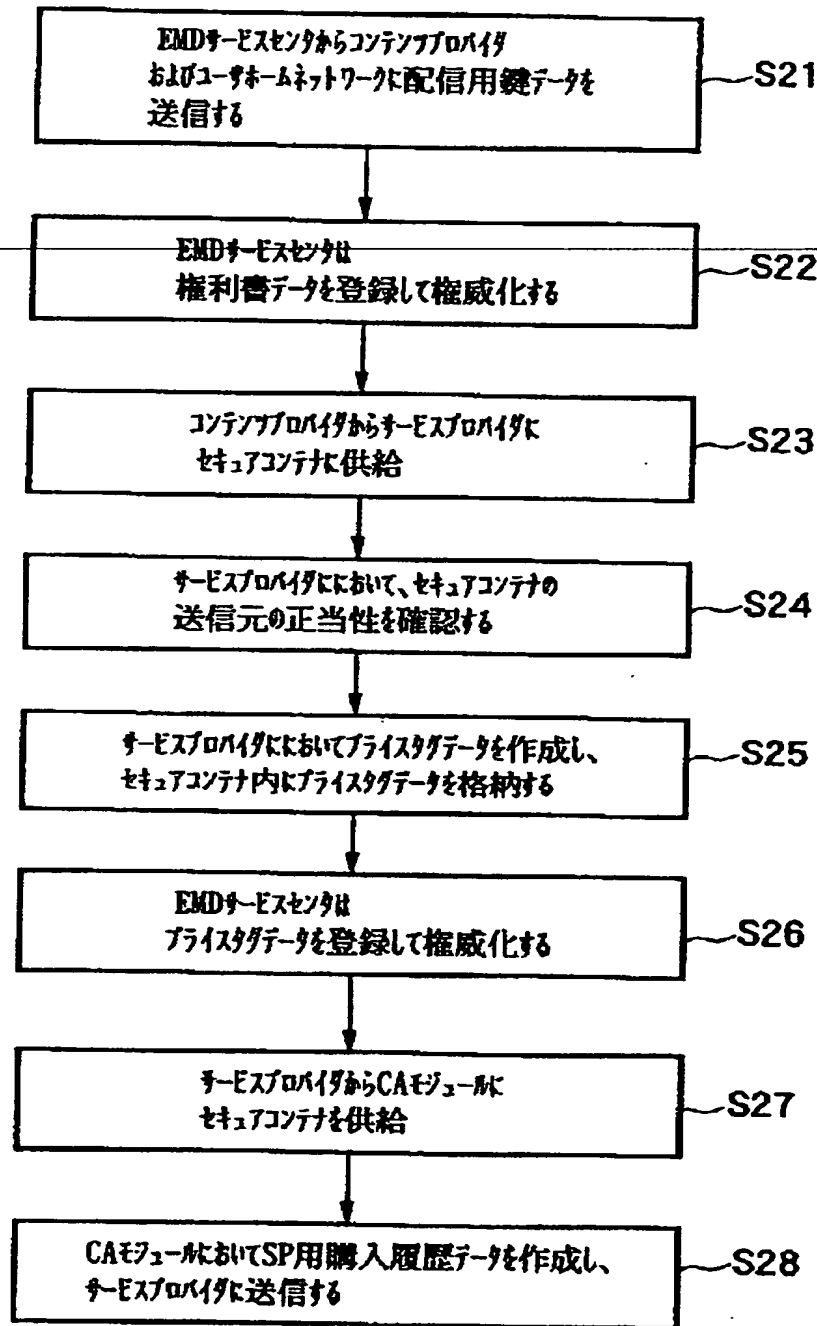
【图 8 2】



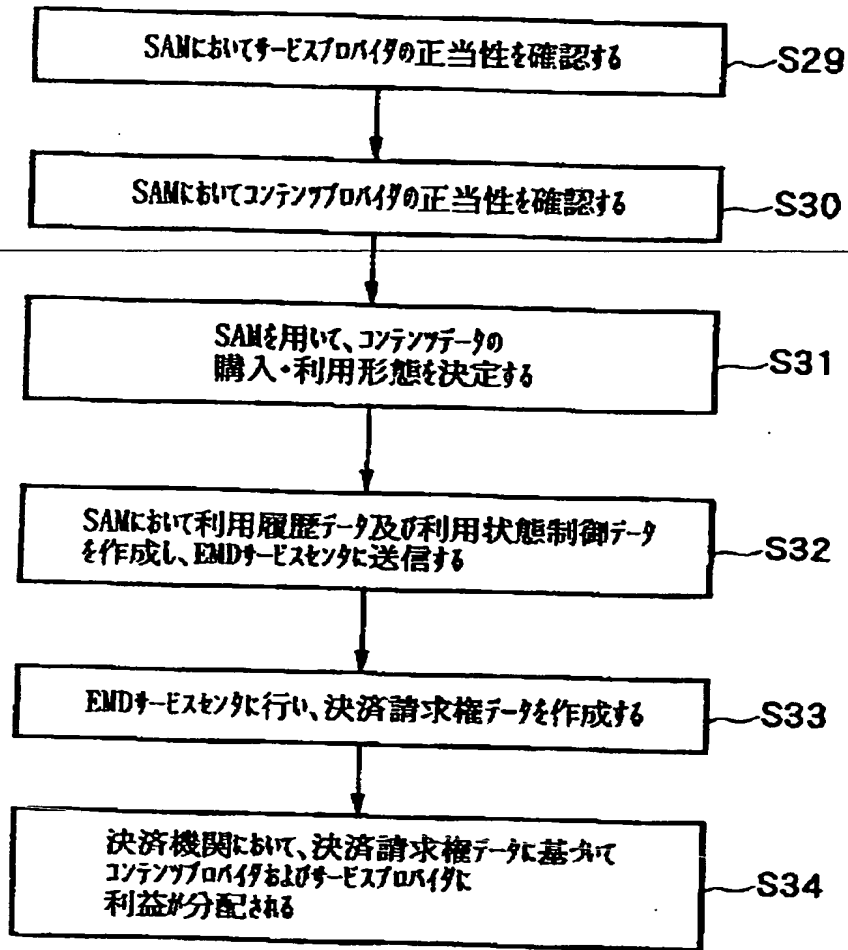
【图 8 3】



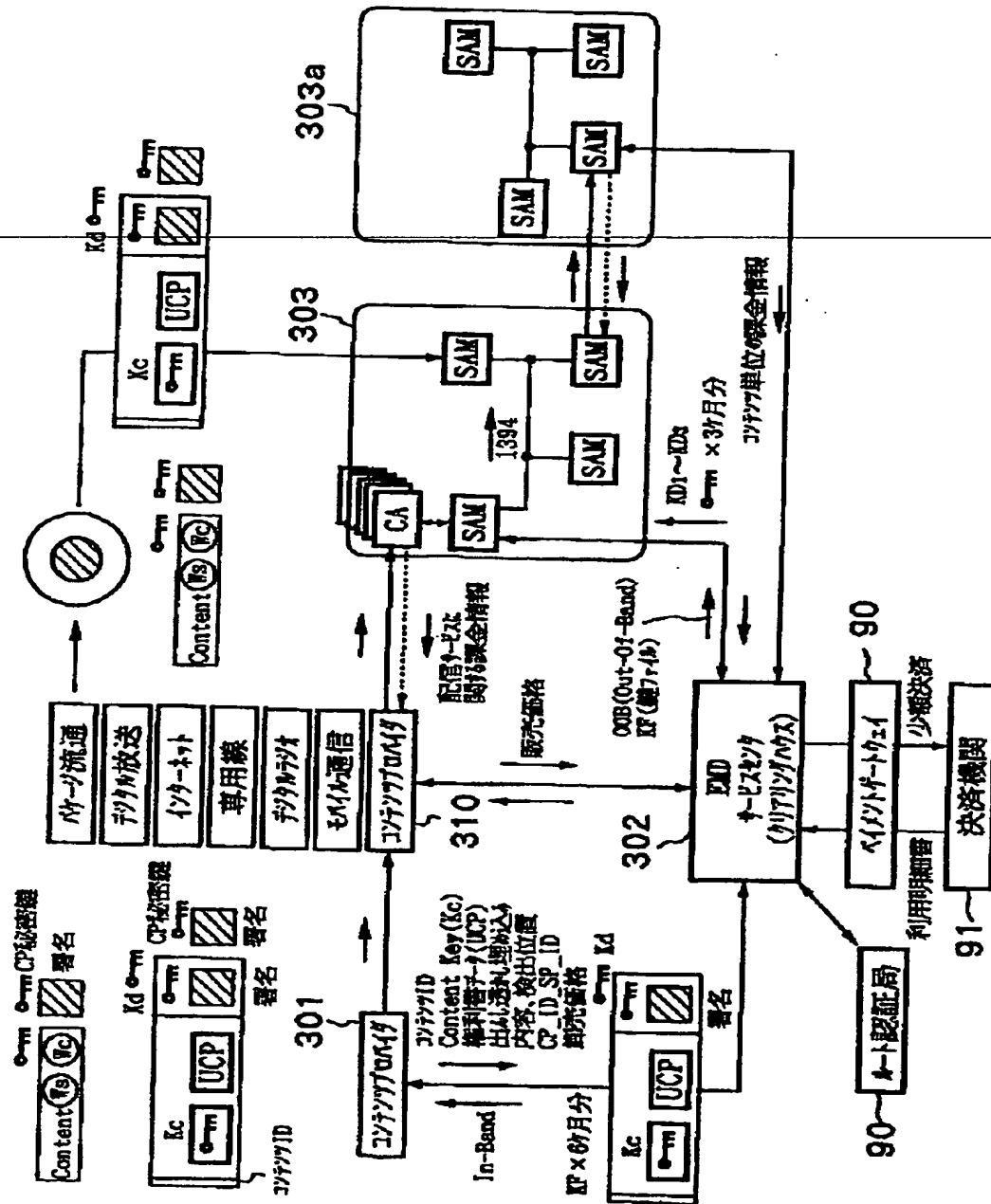
【図 8 4】



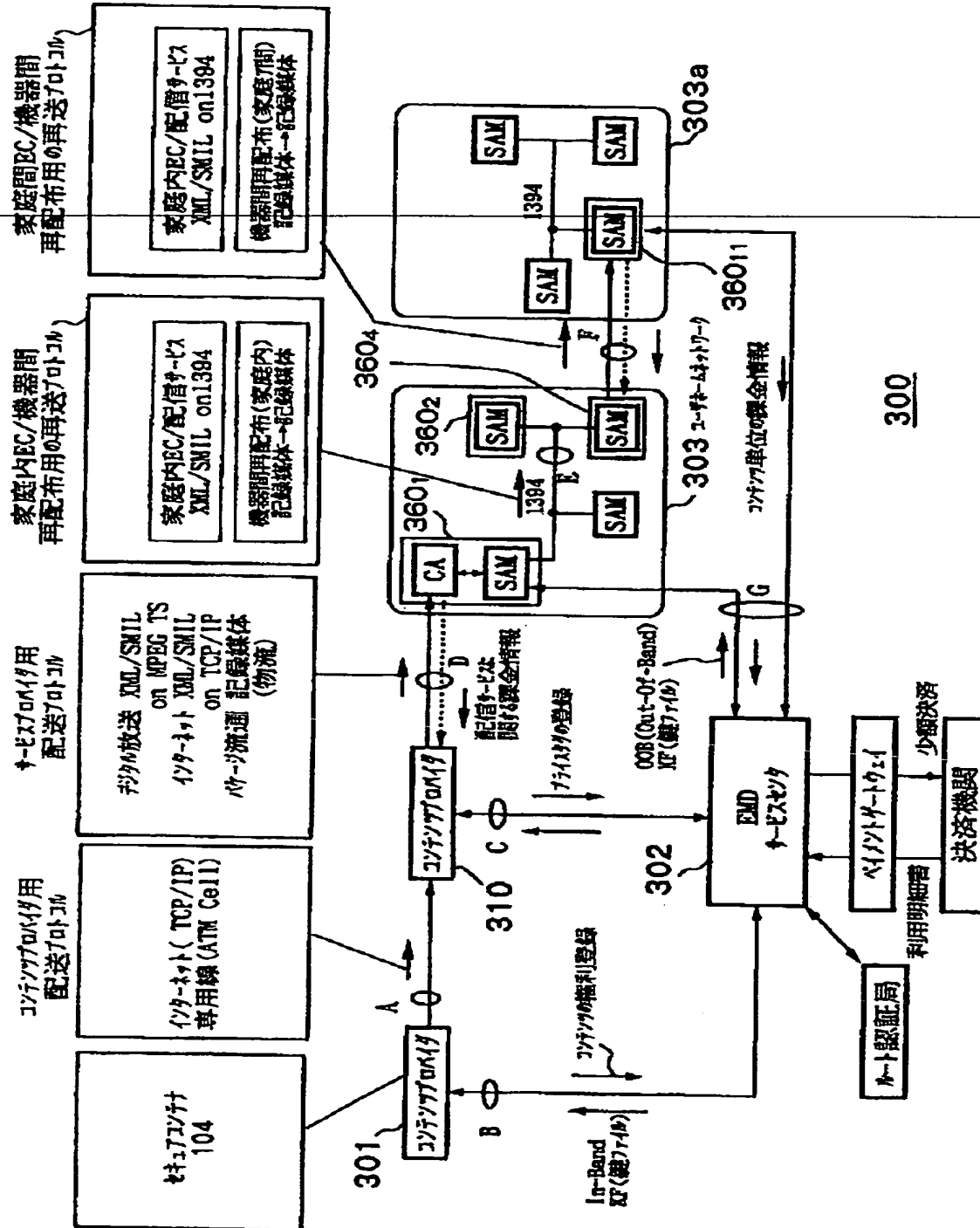
【図 85】



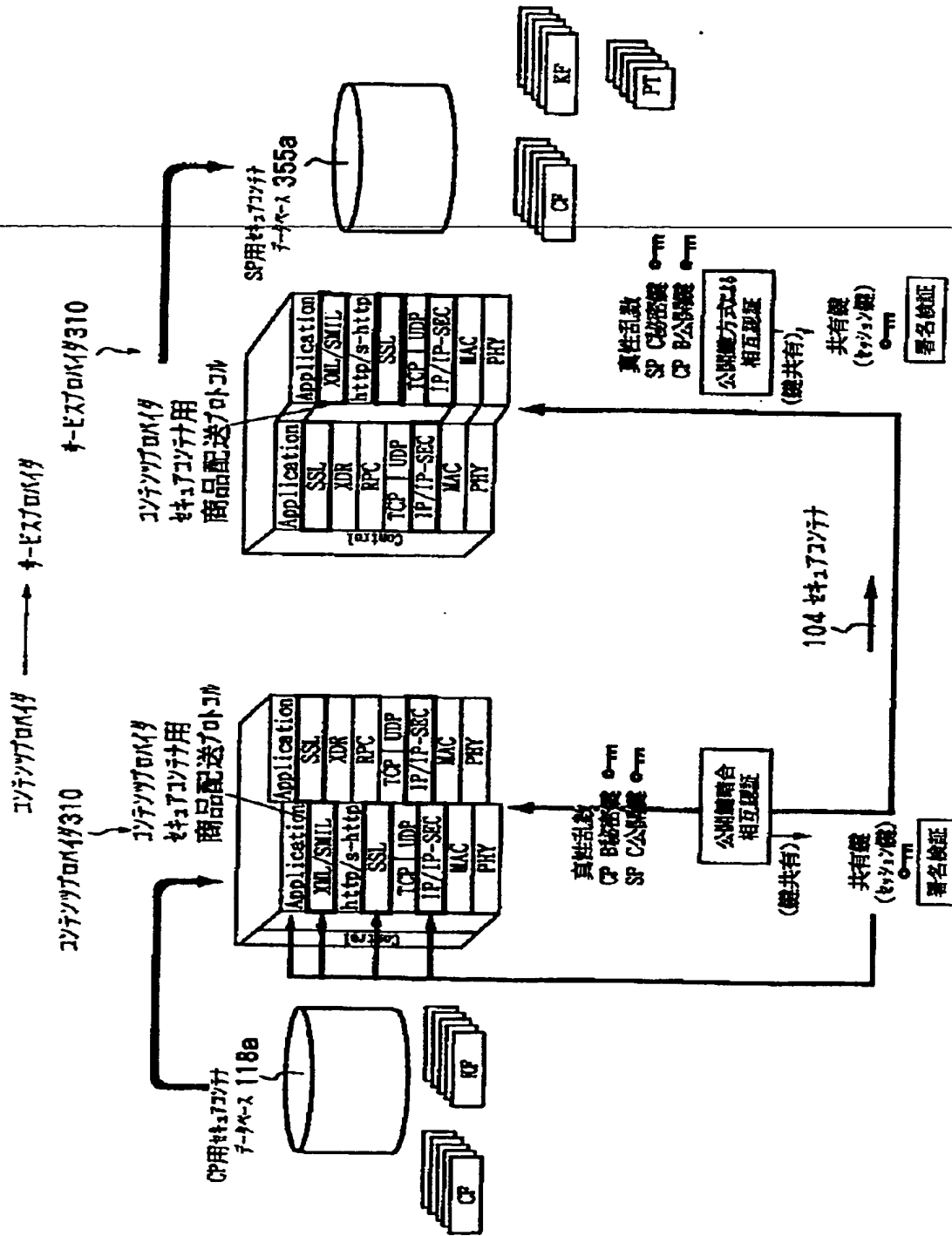
【図 86】



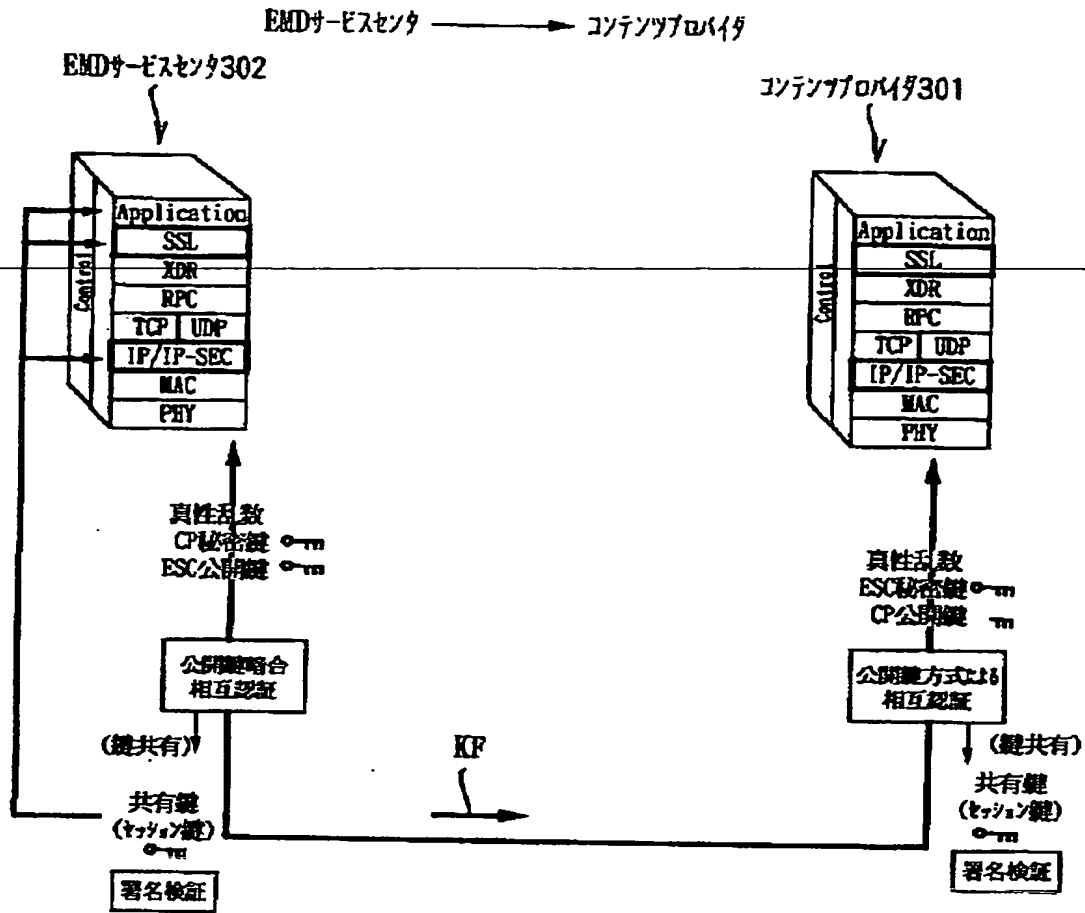
【図 87】



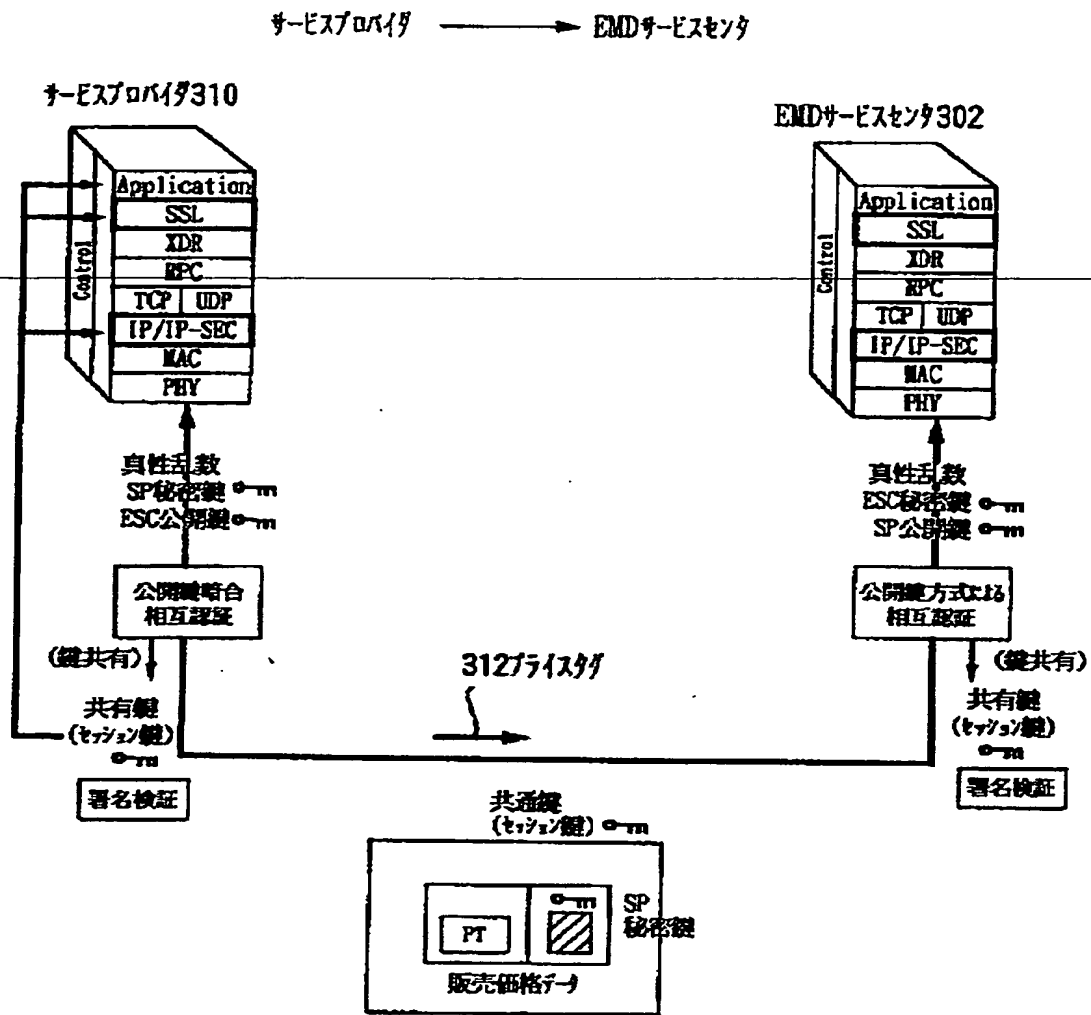
【図 88】

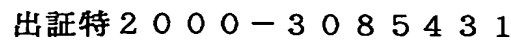


【図 8 9】



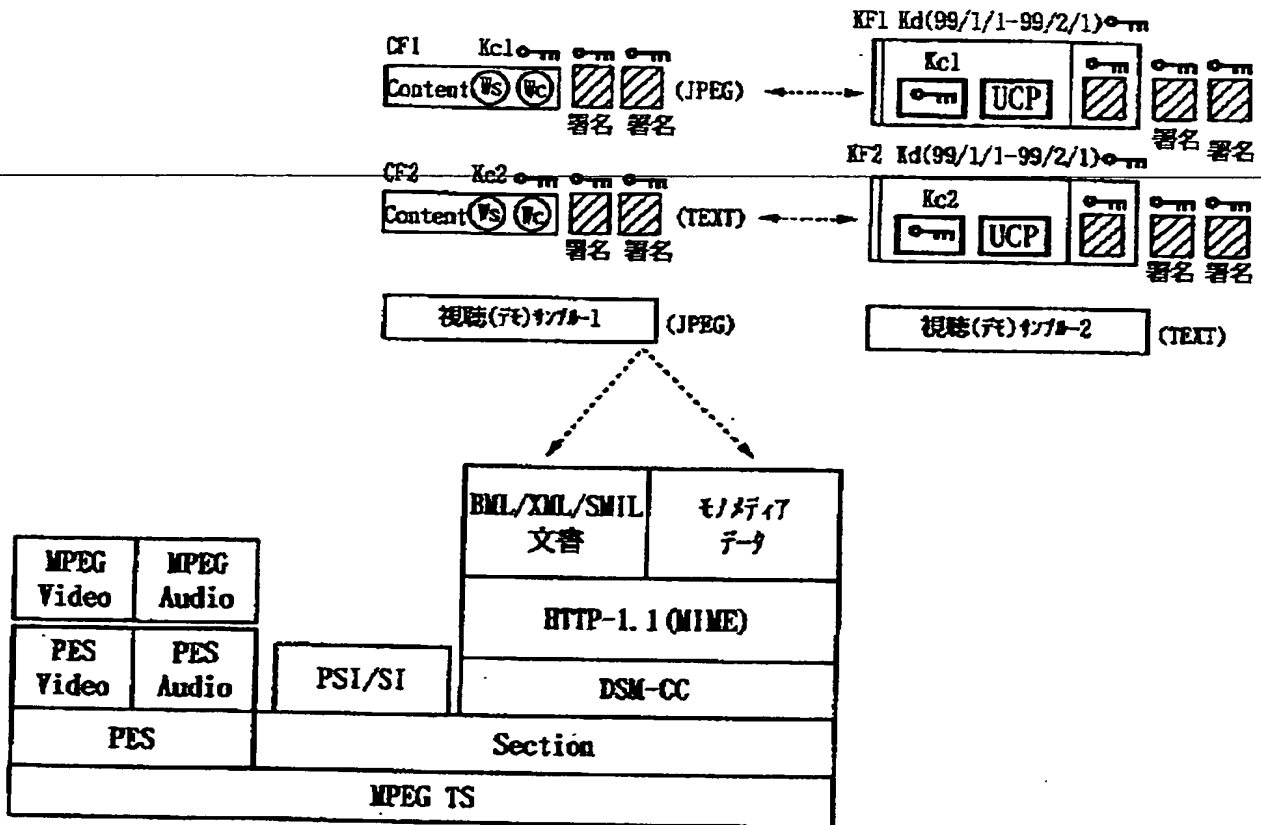
【図 9 0】





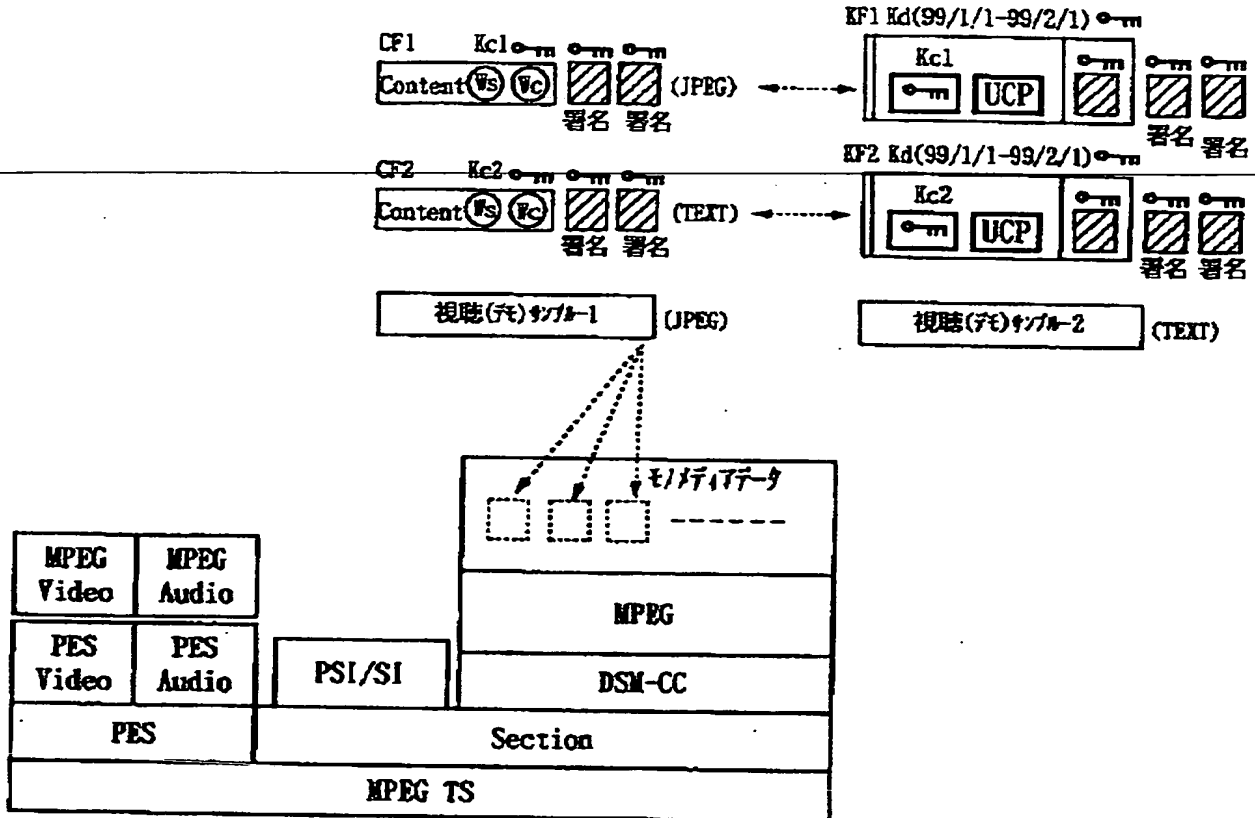
【図 9 2】

デジタル放送のデータ放送方式にXML/SMIL/BMLを利用した場合の
プロトコル階層へのセキュリティコンテナのインテグリティ



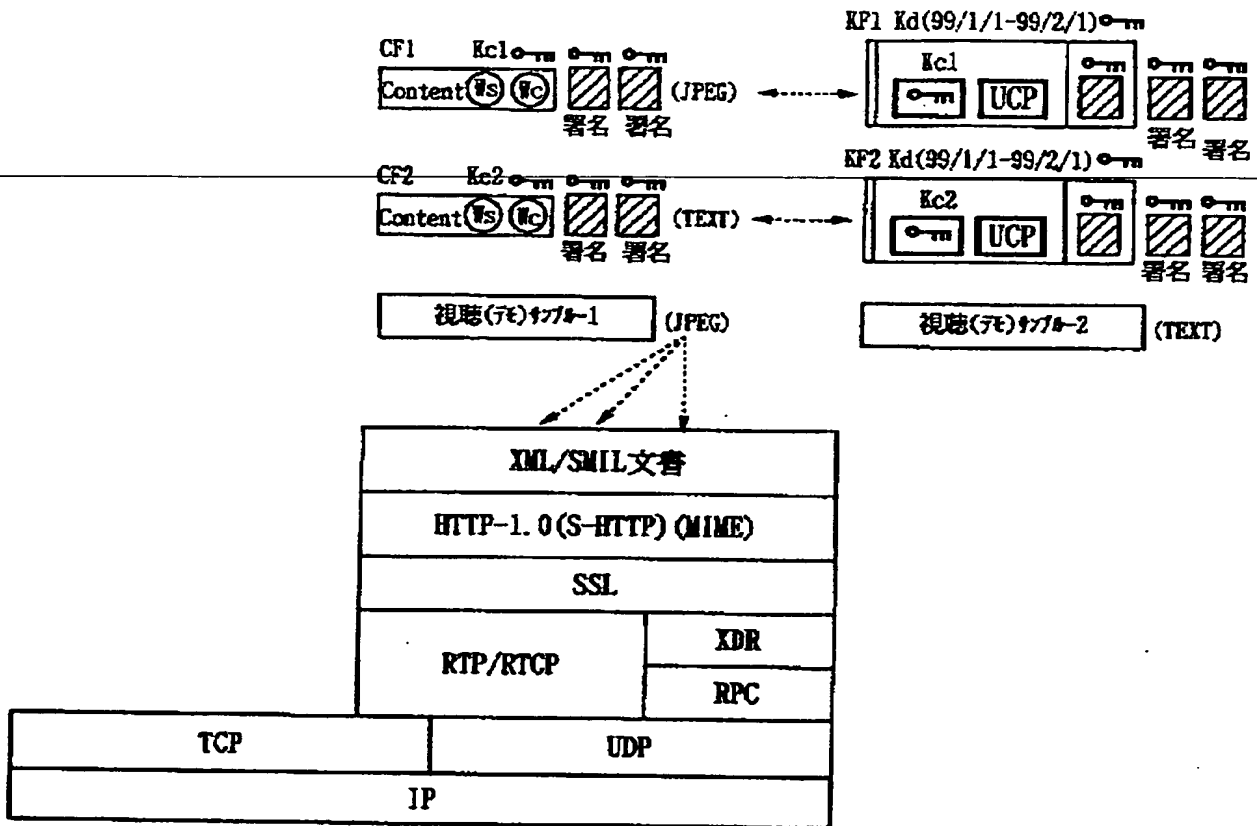
【図 9 3】

デジタル放送のデータ放送方式にMPEGを利用した場合の
プロトコル階層へのセキュリティ要素のインテグリティ

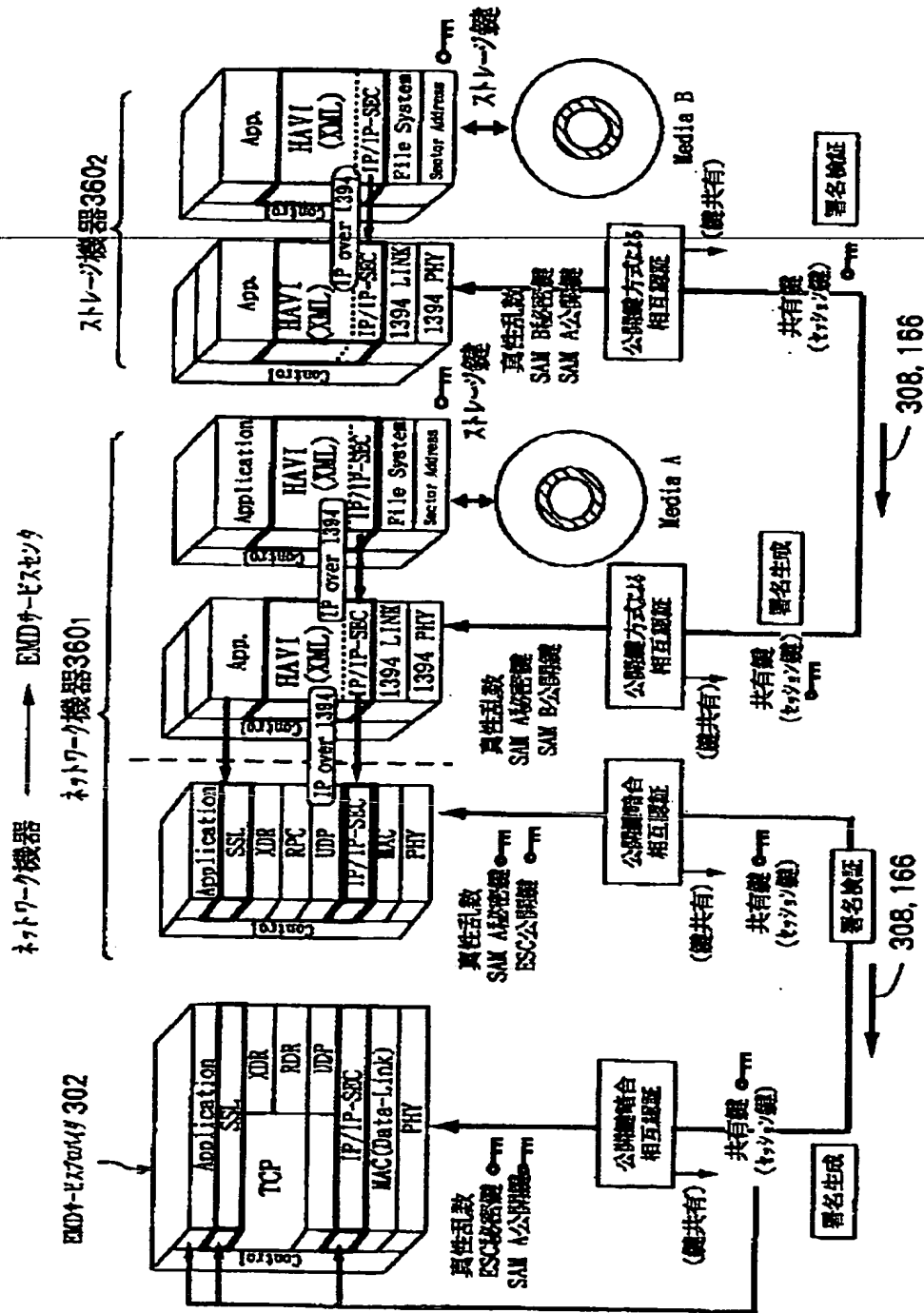


【図 9 4】

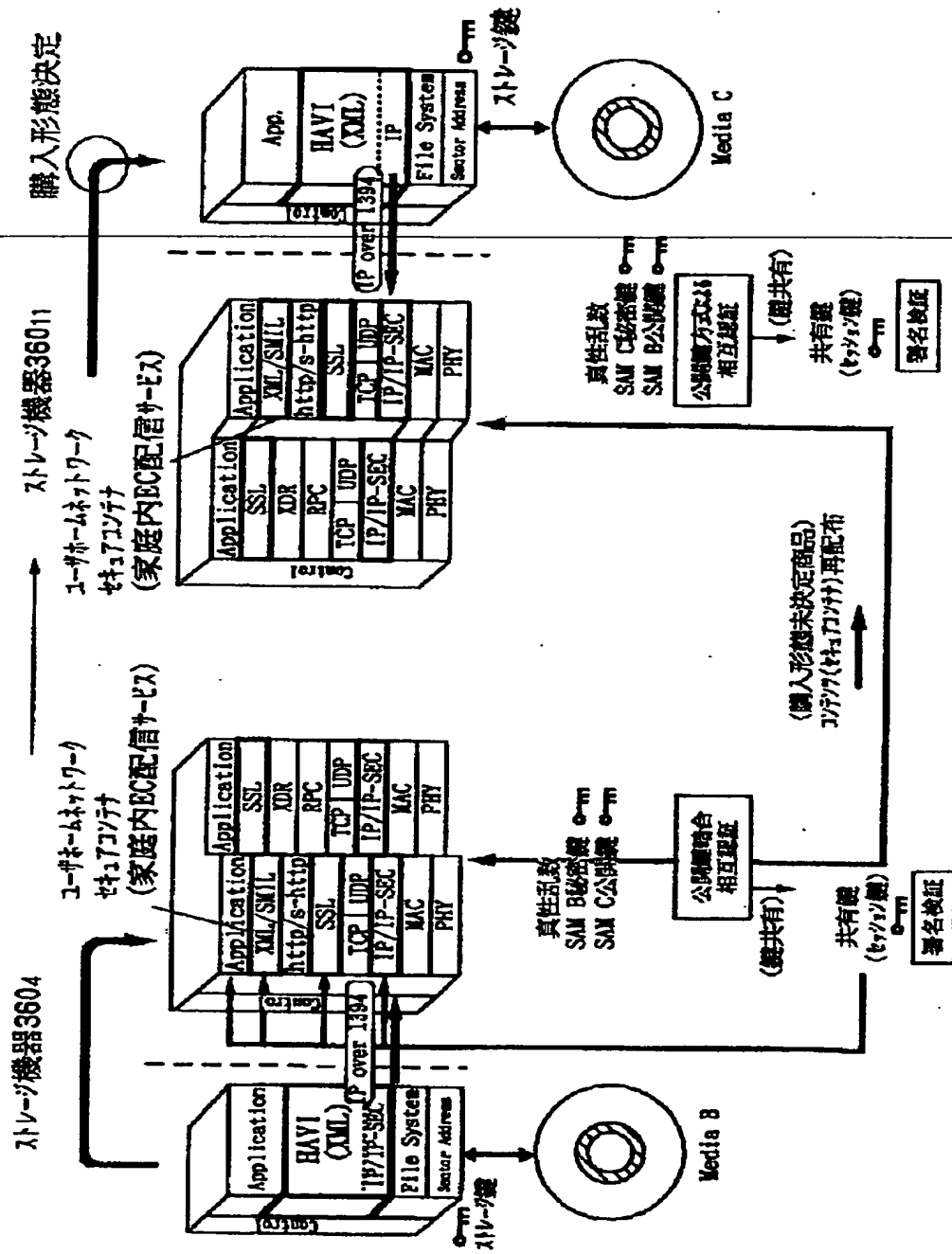
インターネットのデータ放送方式にXML/SMILの
プロトコル階層へのセキュリティのインクリメント



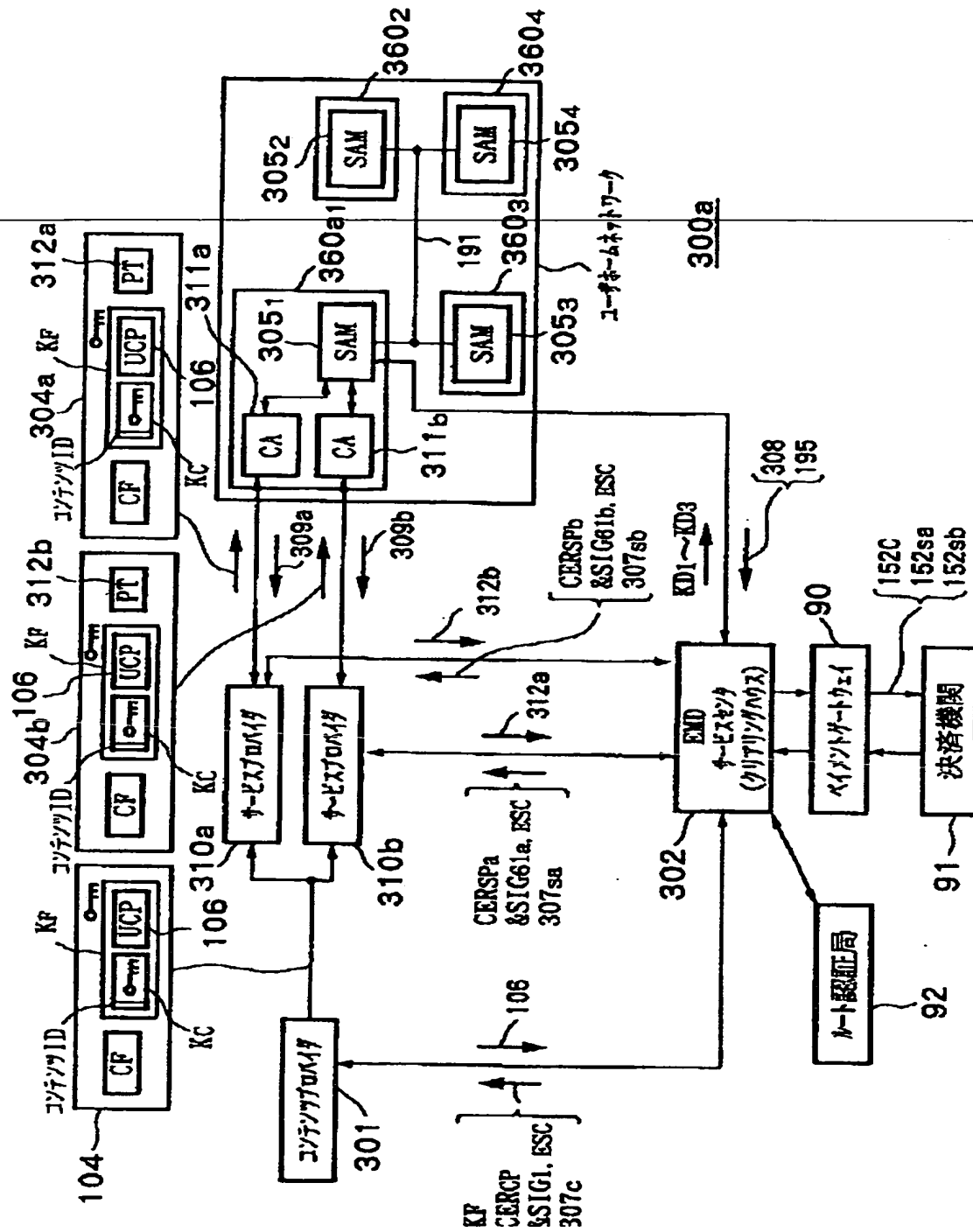
【図 95】



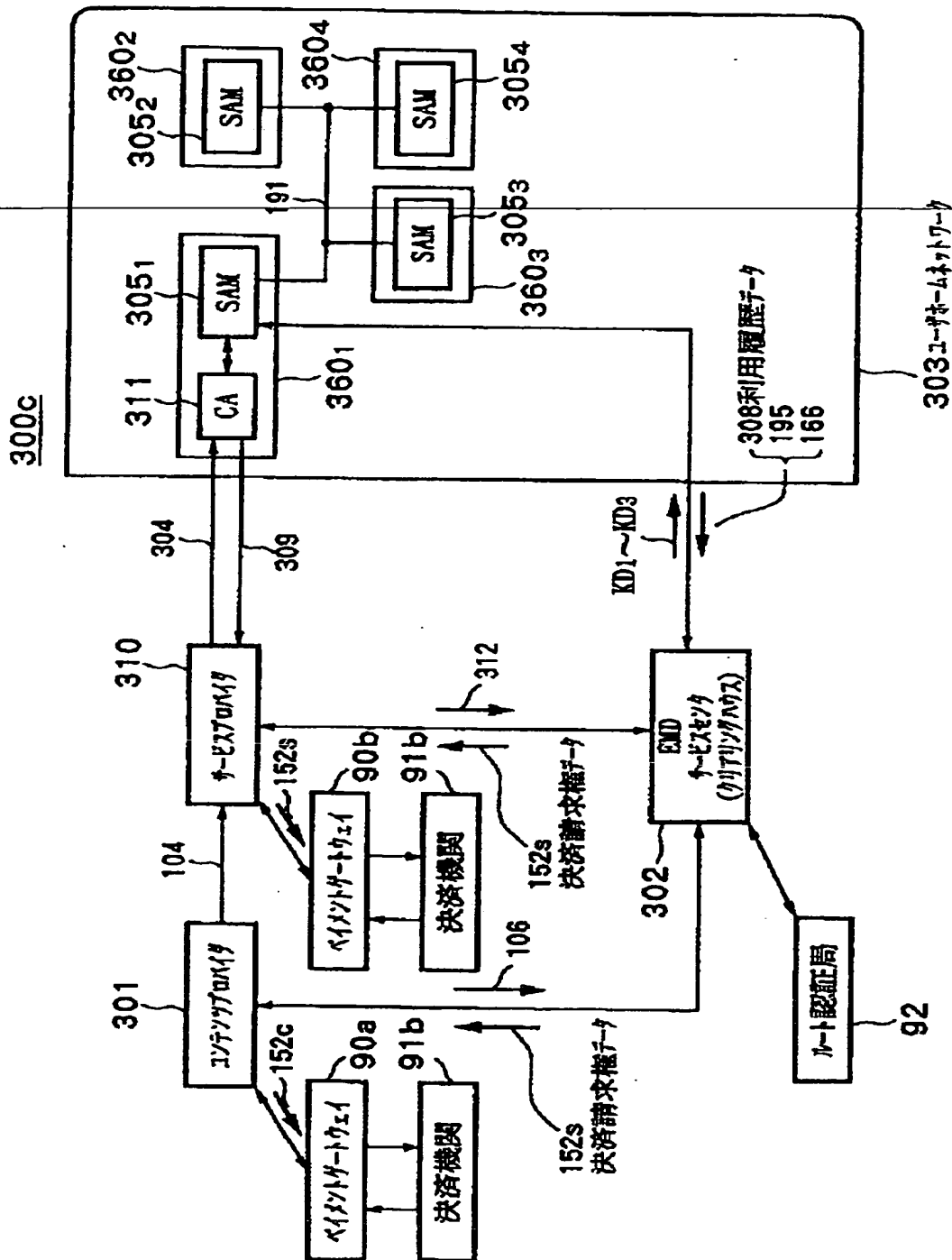
【図 96】



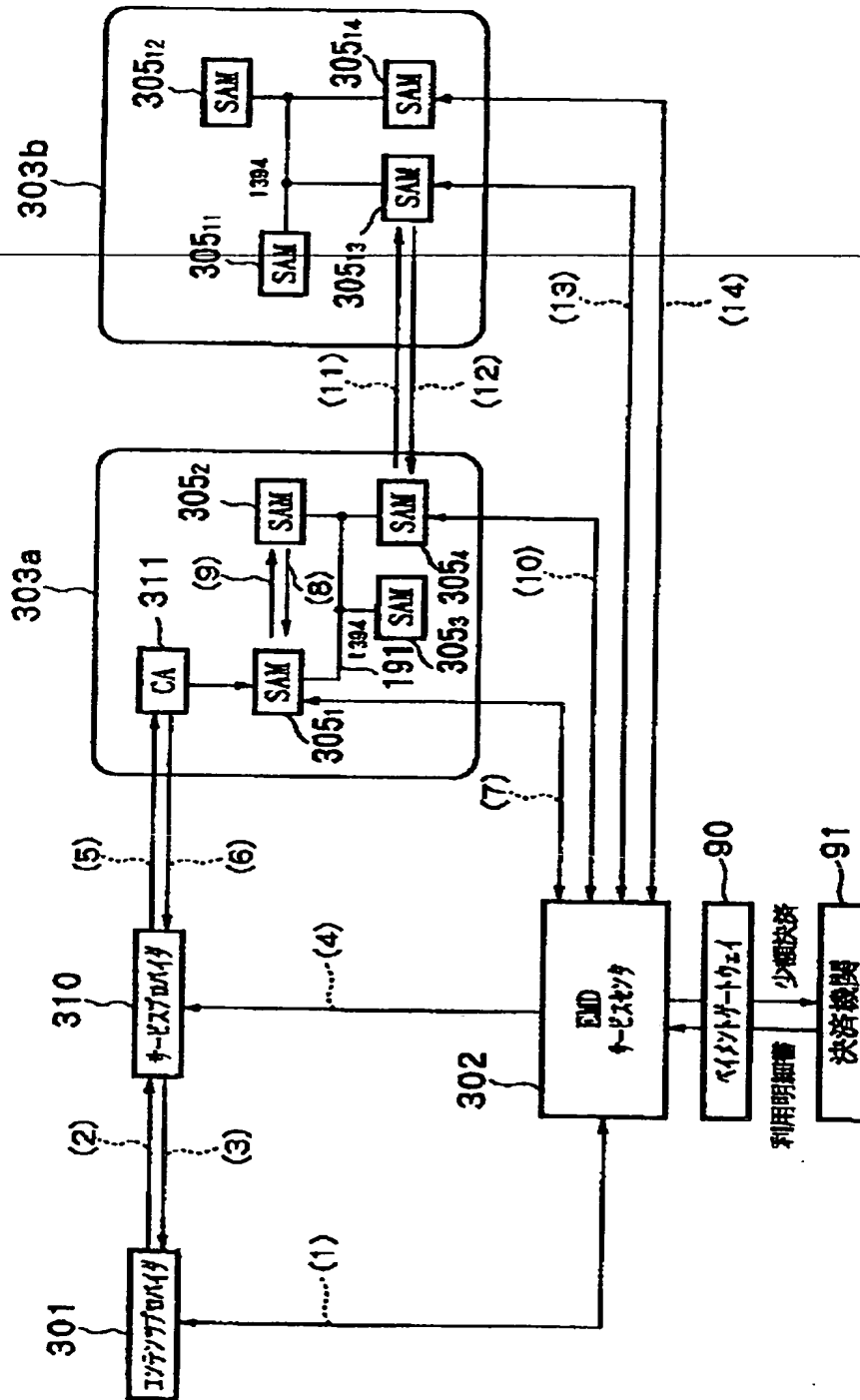
【図 97】



【图 9 9】

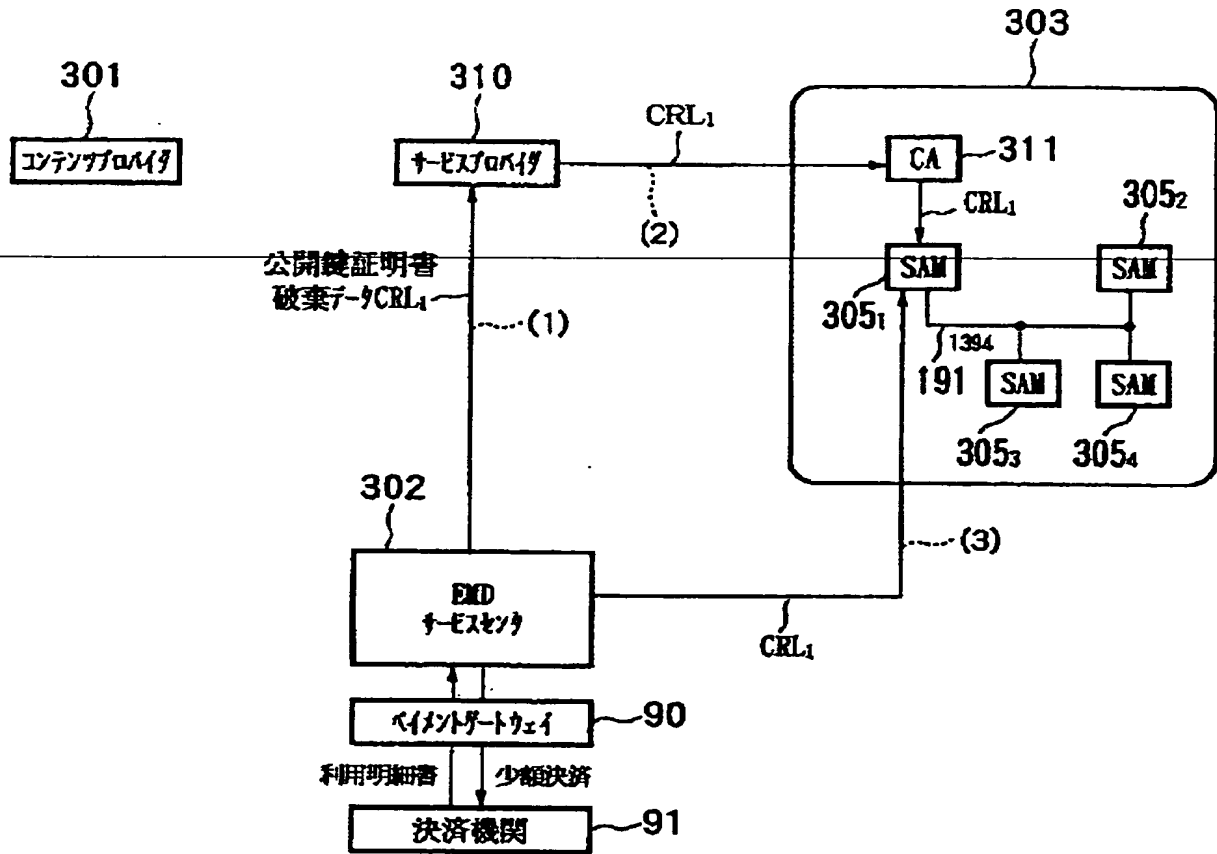


【図 1 0 1】



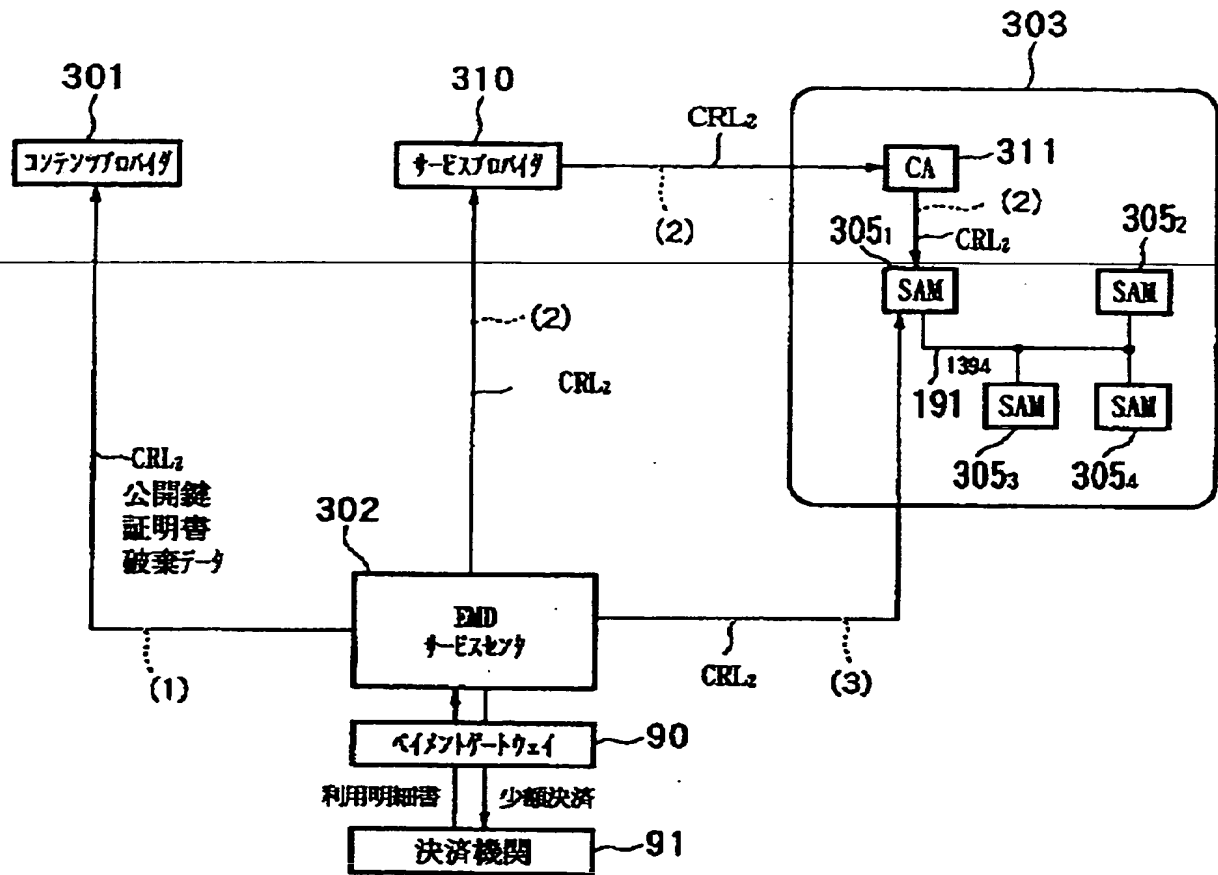
公開鍵証明書の手続

【図 1 0 2】



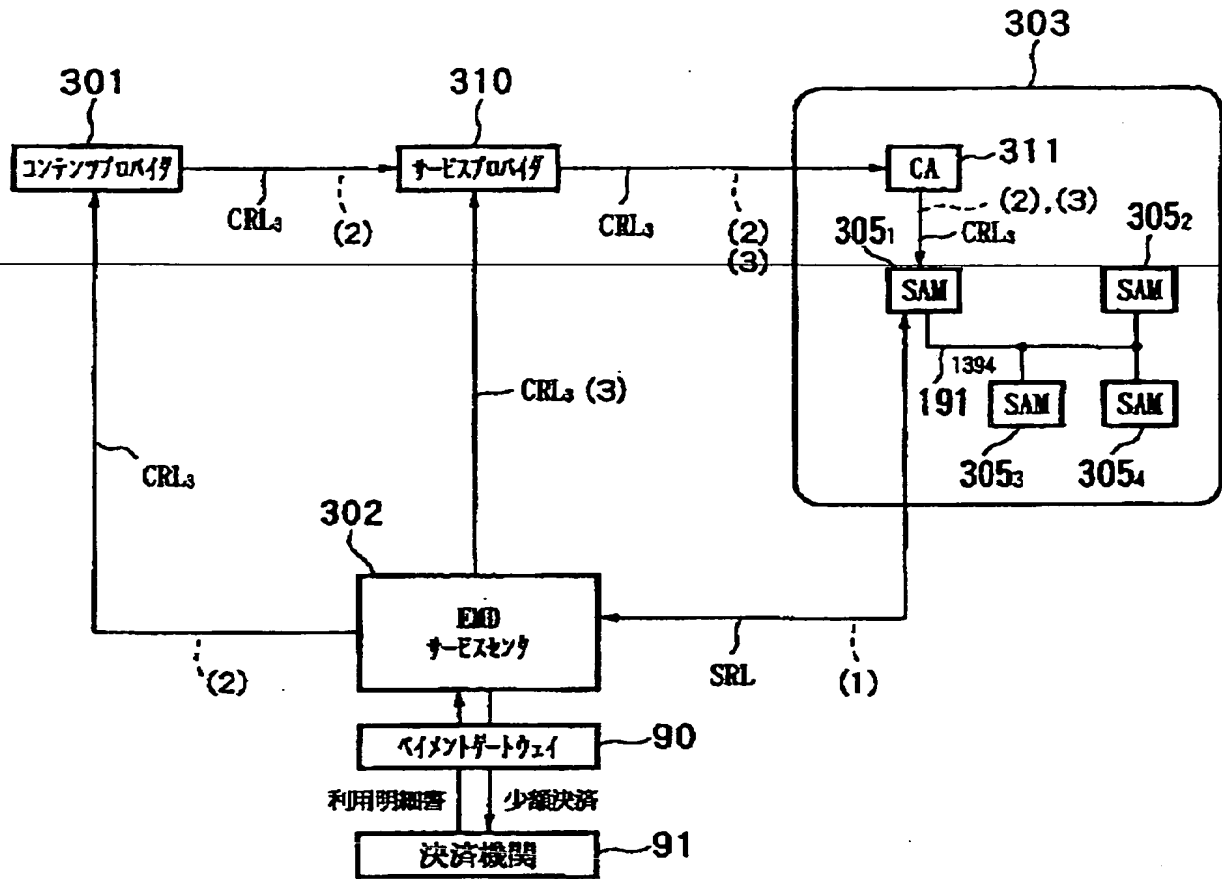
CER_{CP}を無効にする場合

【図 103】

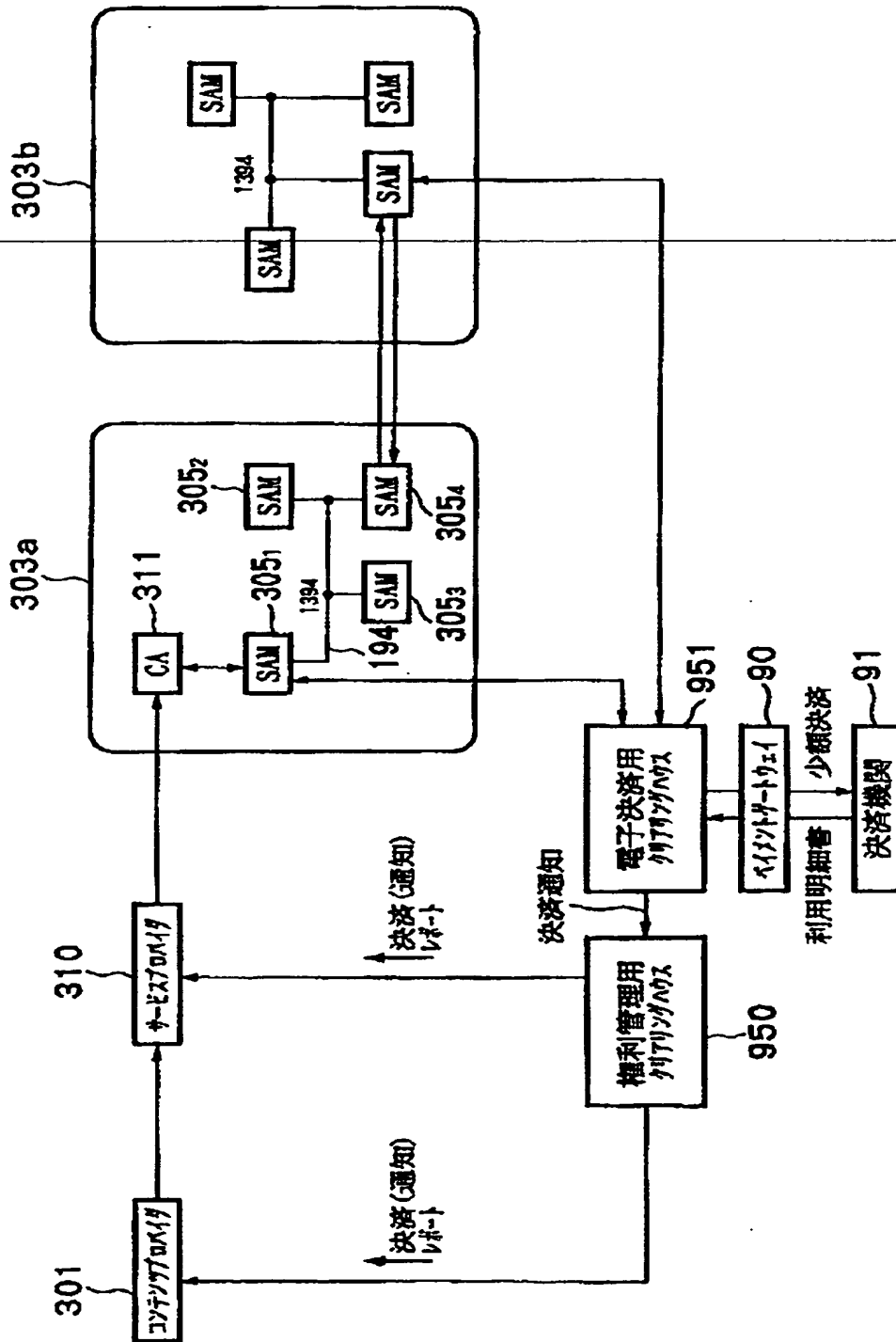


CERsが無効になる場合

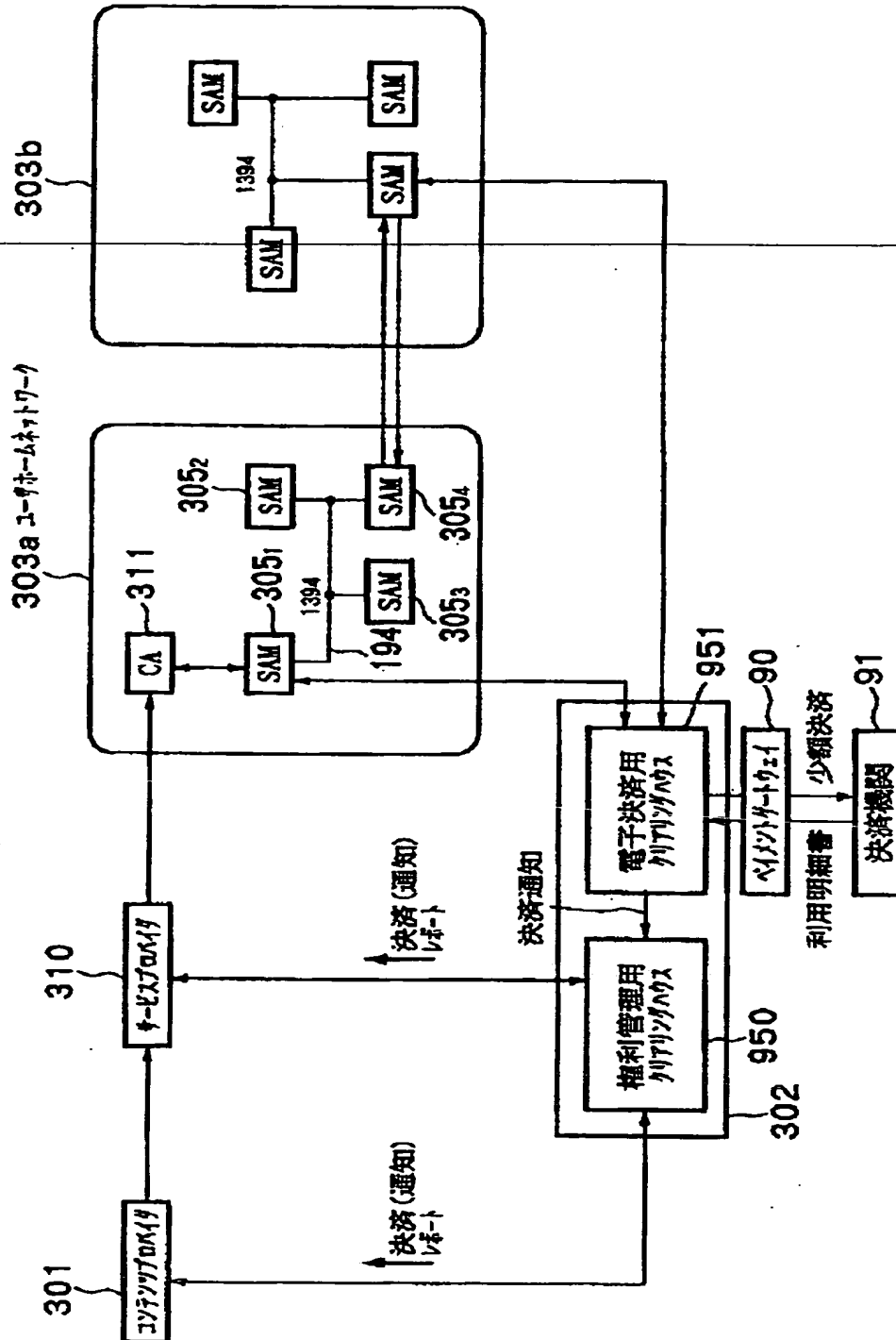
【図 1 0 5】



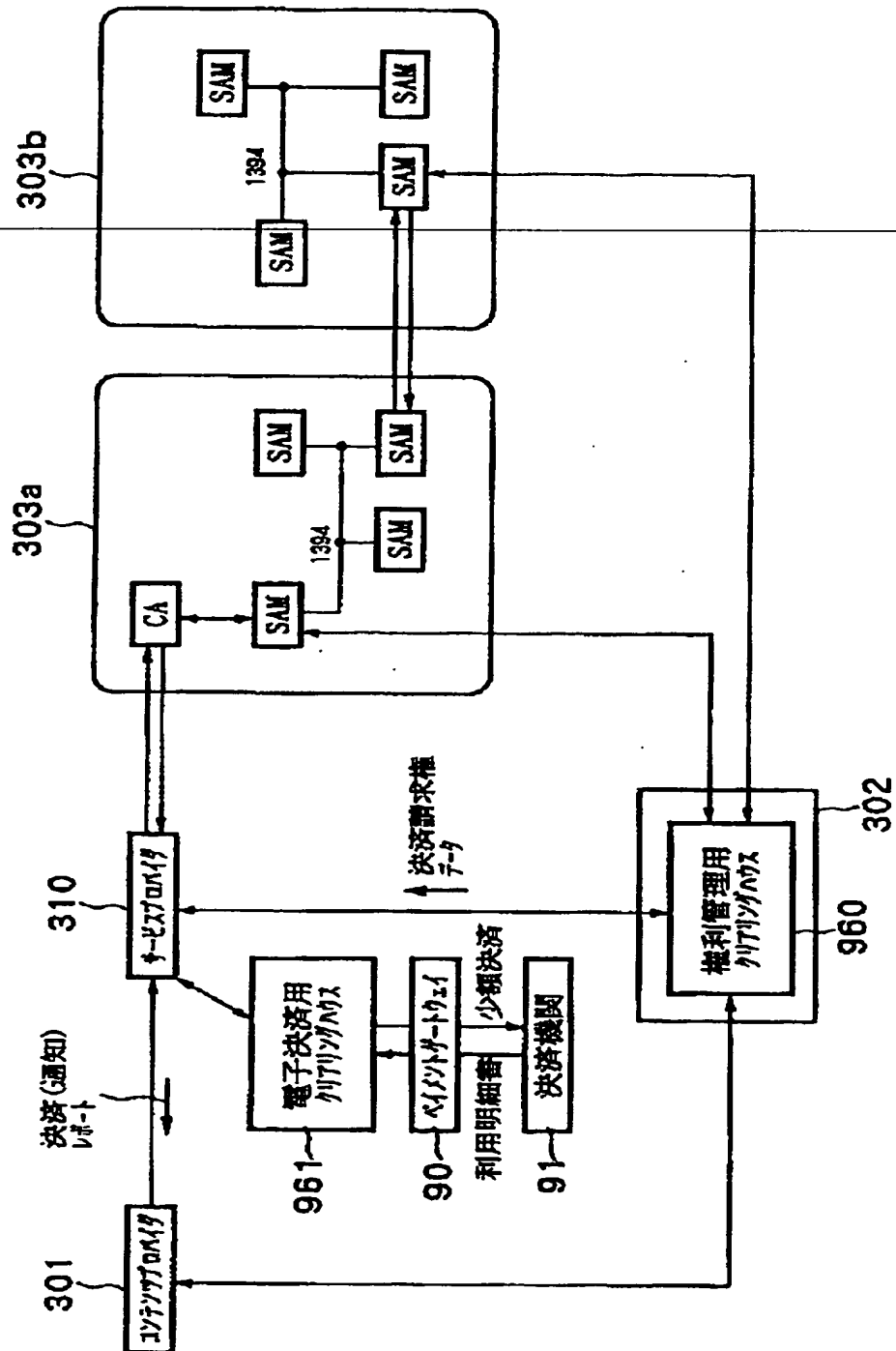
【図 1 0 6】



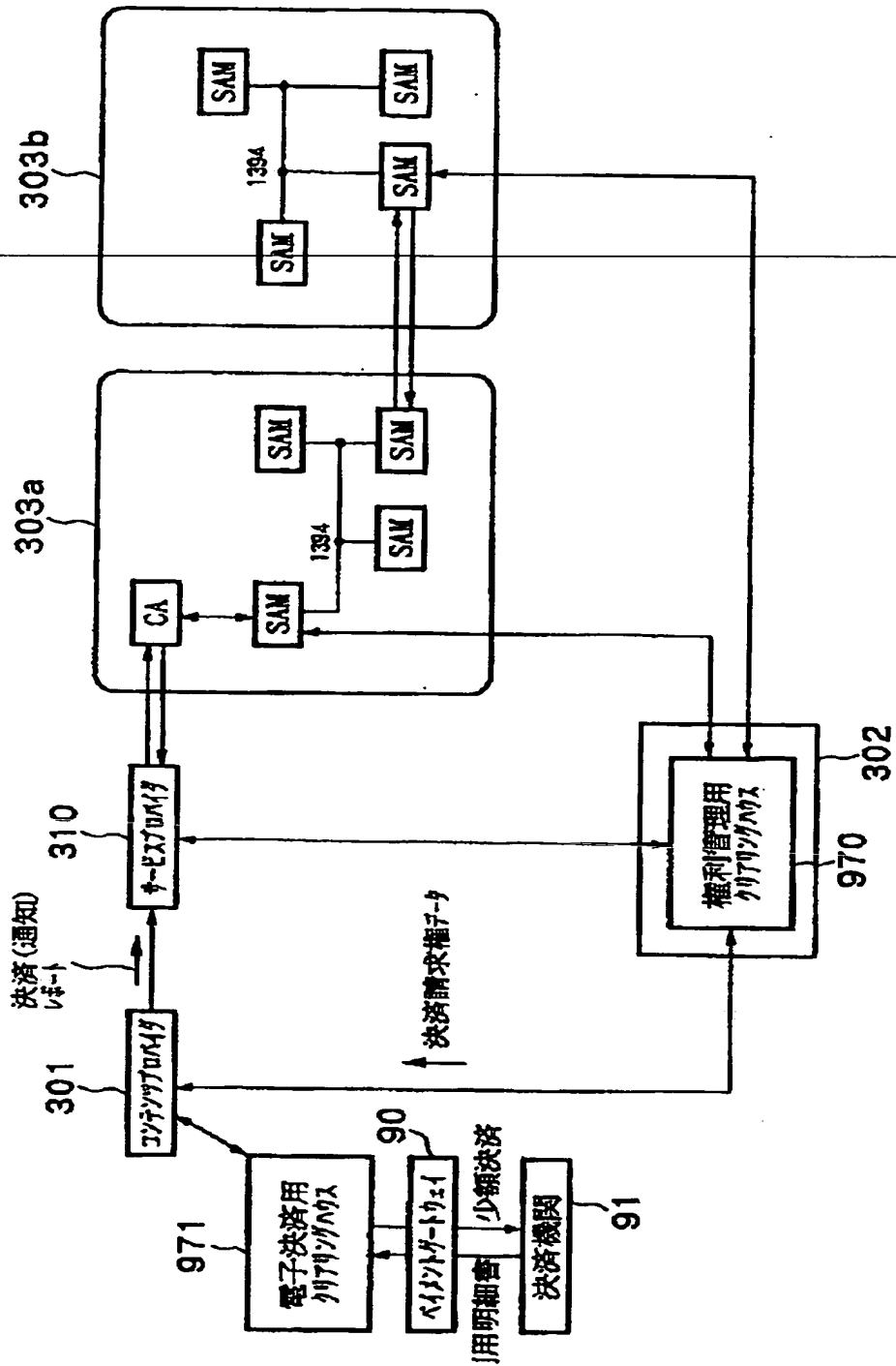
【図 107】



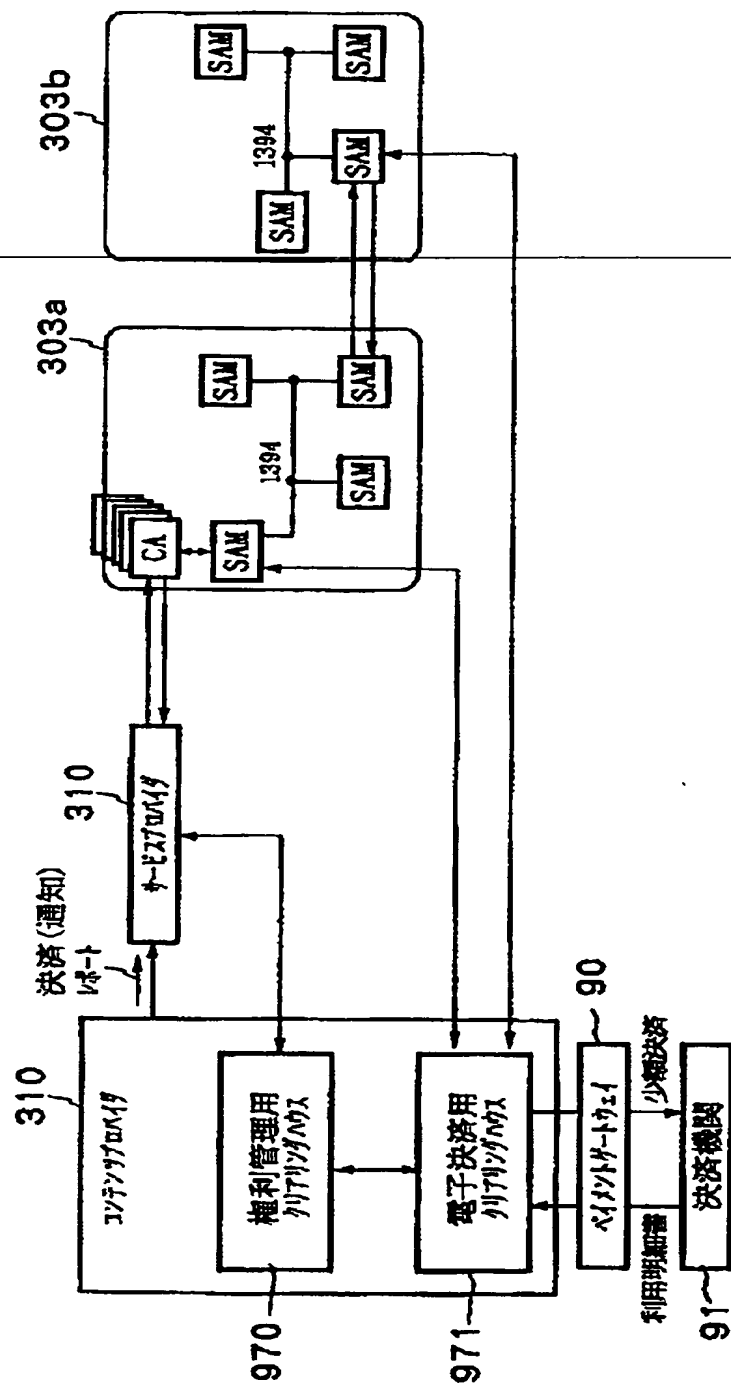
【図 1 0 8】



【図 109】

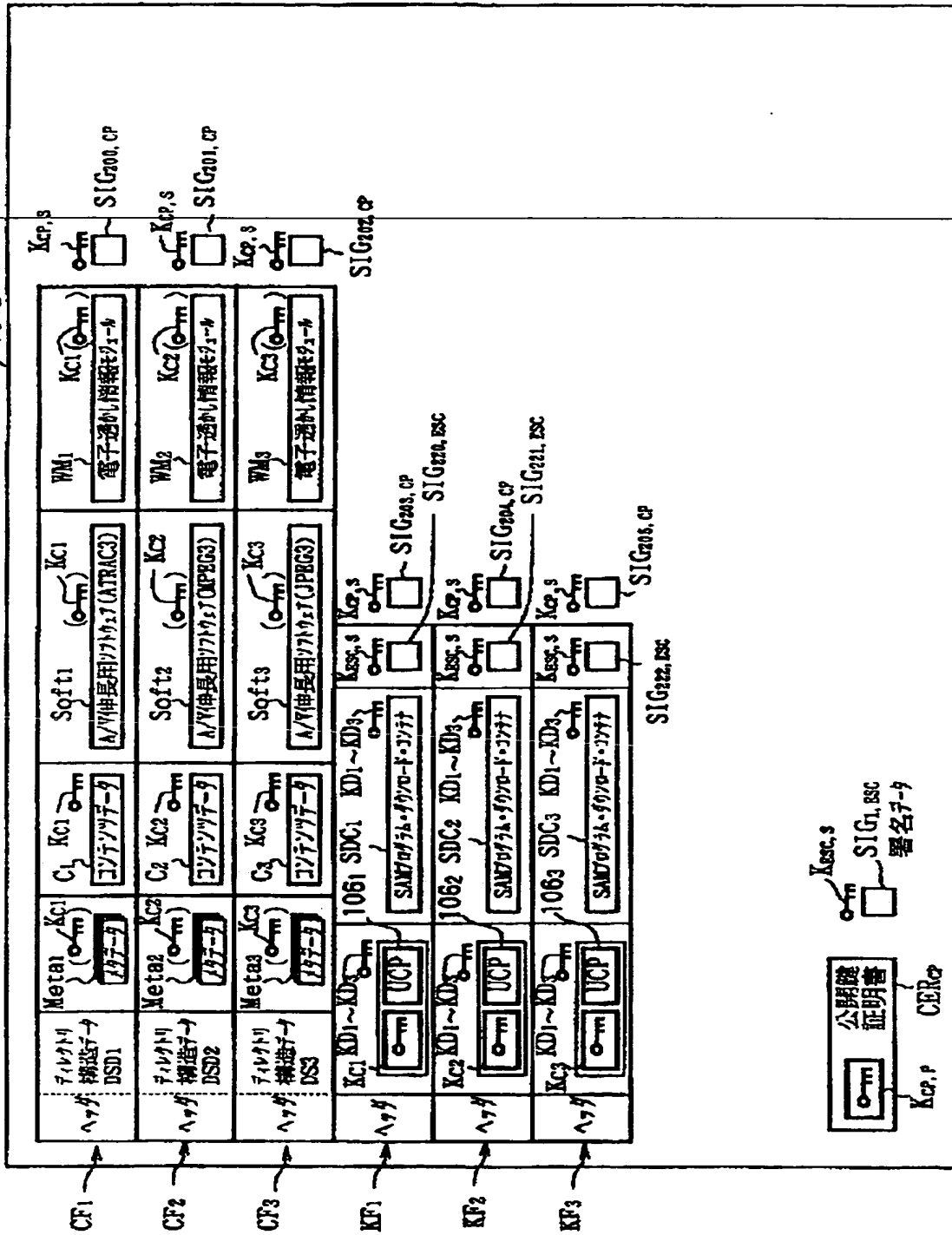


【図 1 1 0】

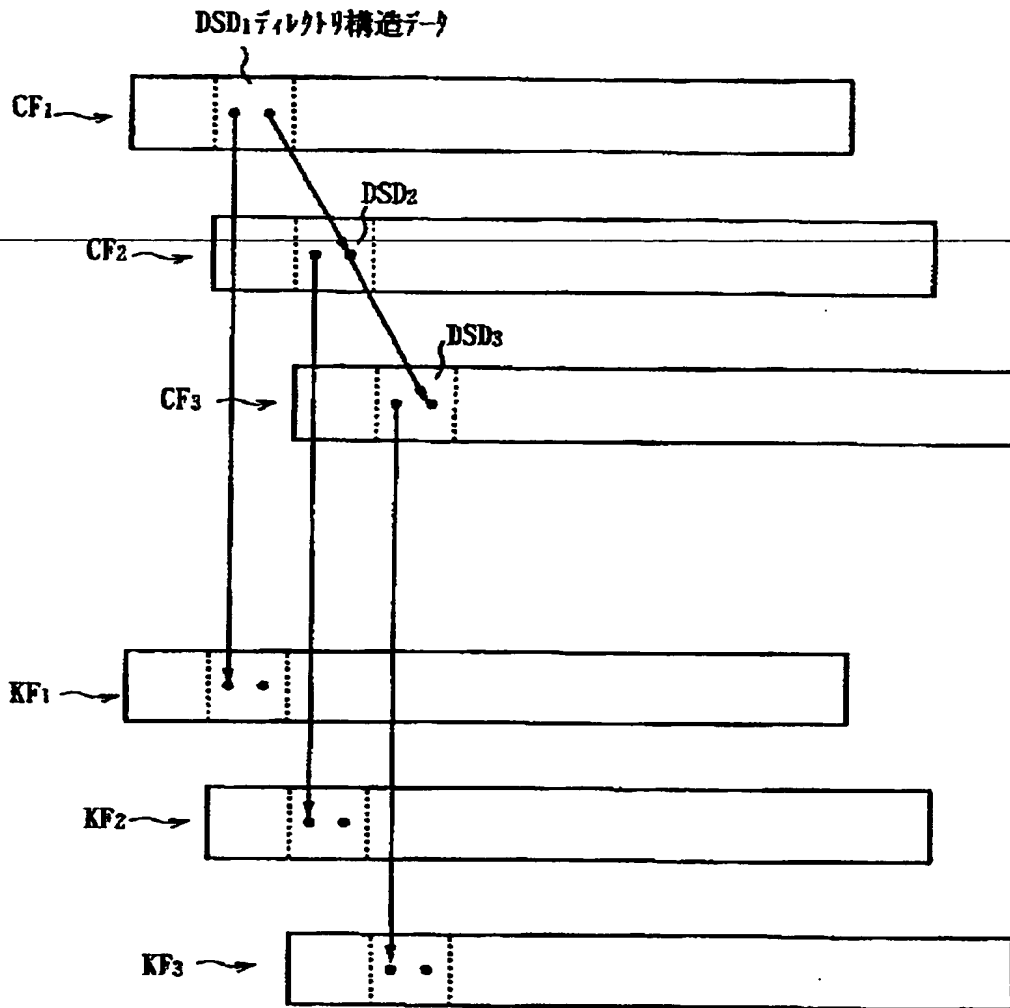


【図 111】

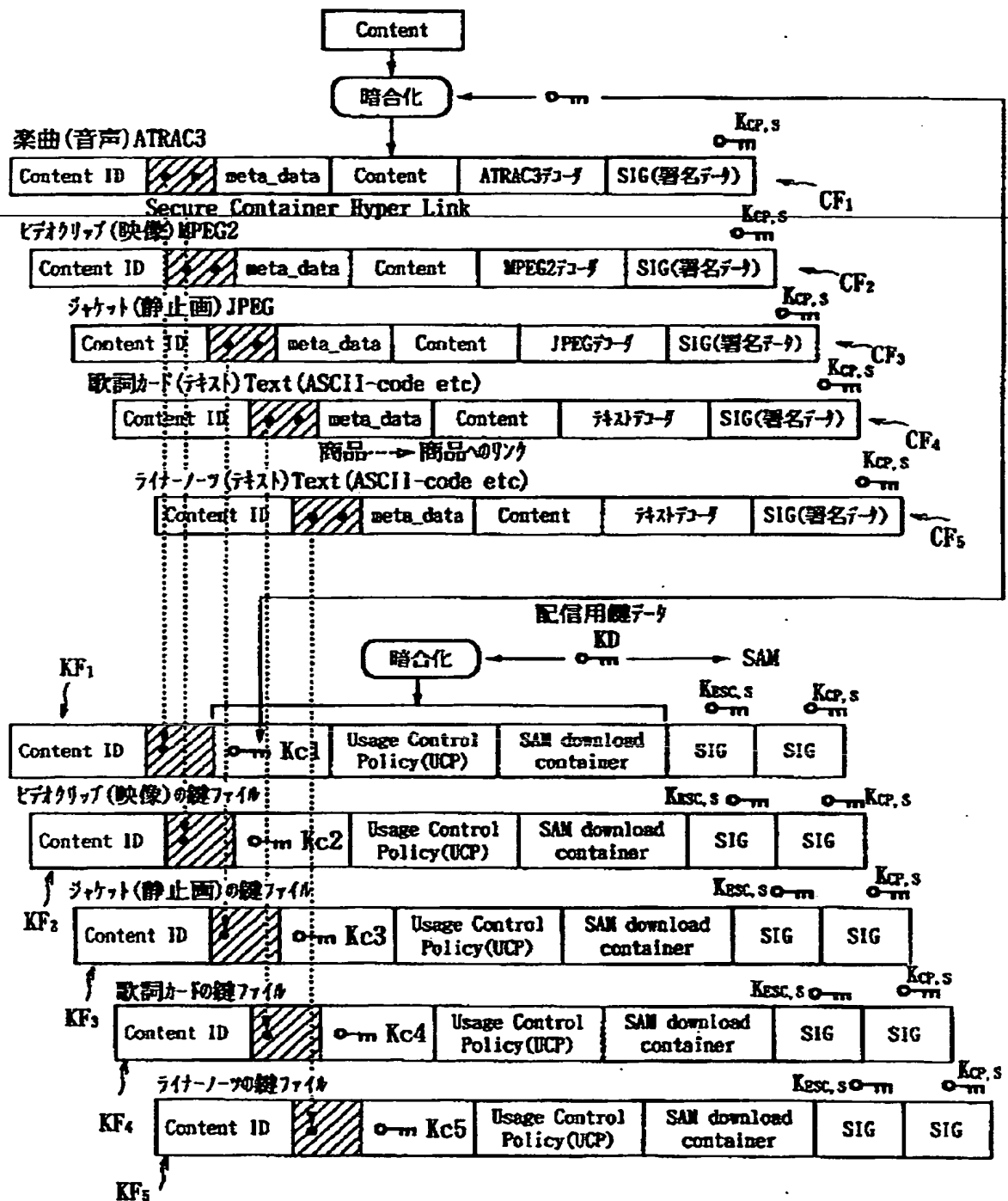
104a 拡張コネクタ



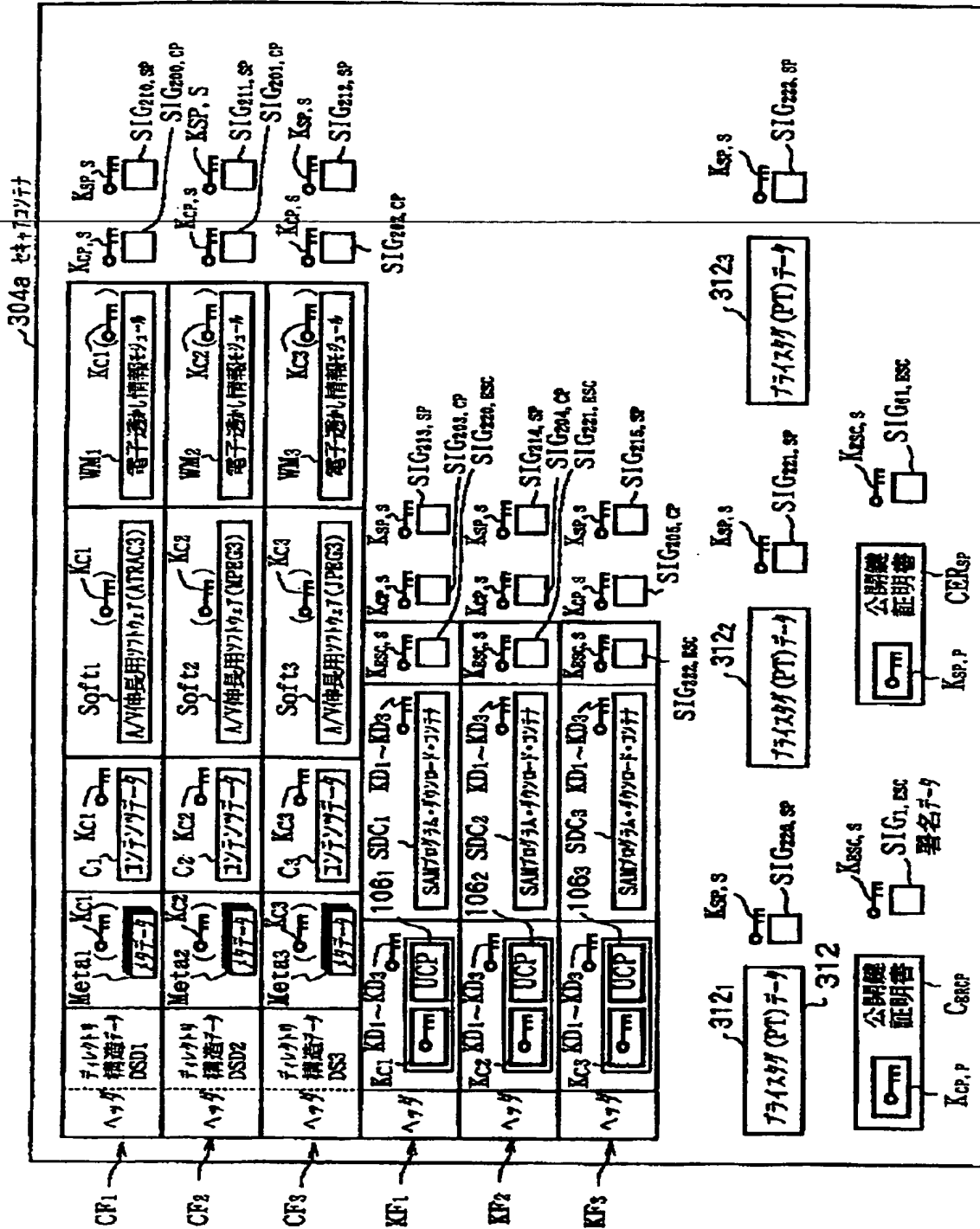
【図 1 1 2】



【図 113】



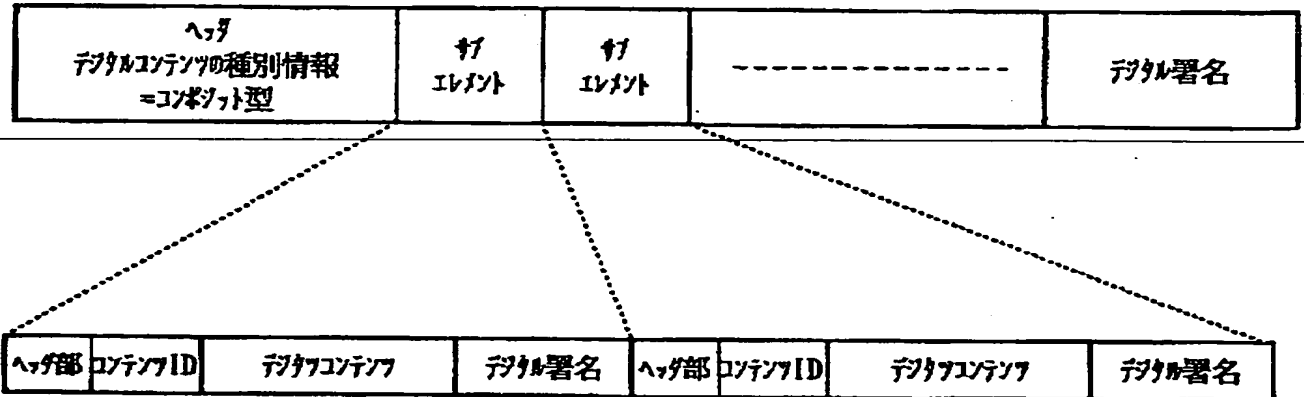
【図 114】



【図 115】

セキュアコンテンツ(コンポジット型)のデータフォーマット①

基本構成

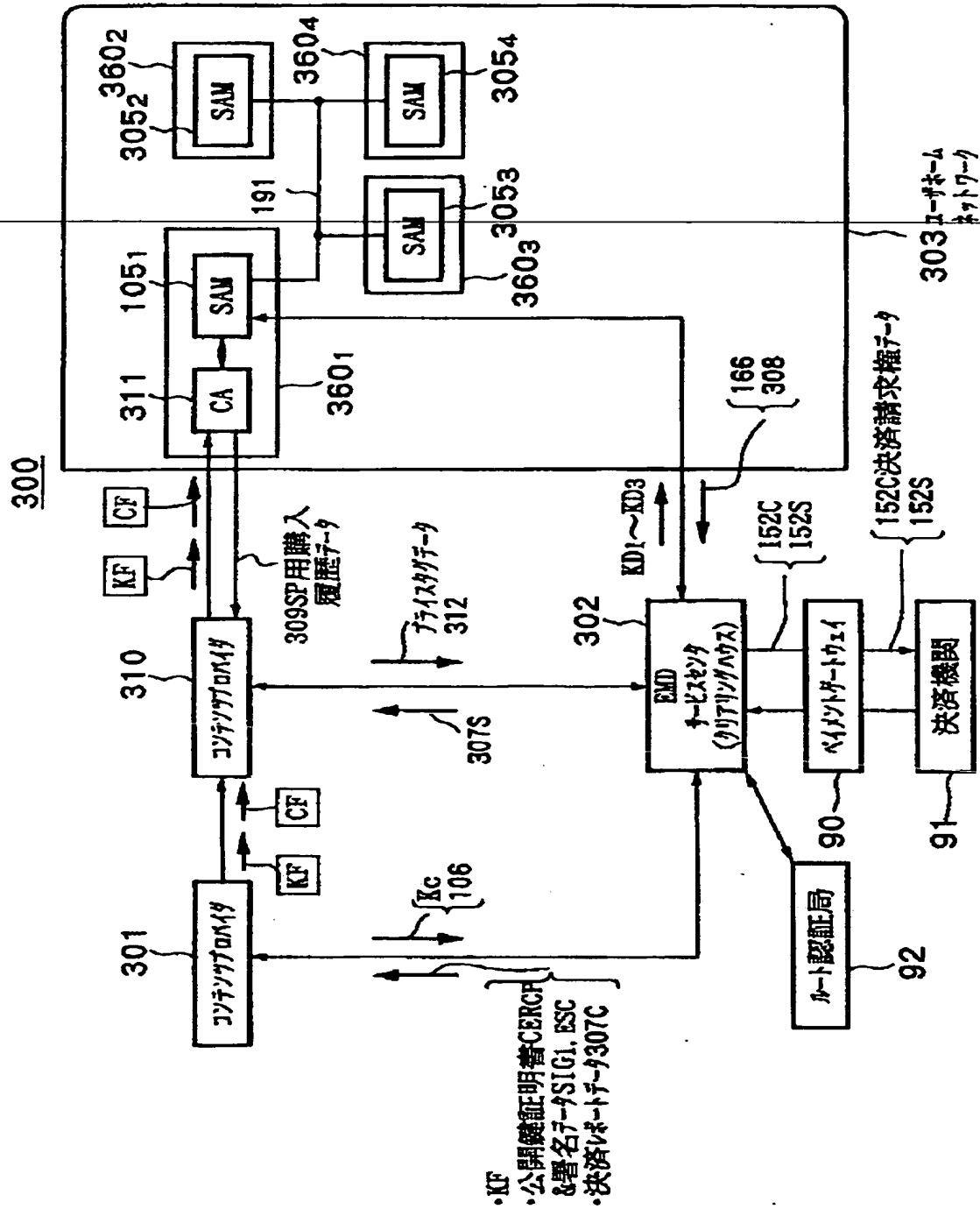


【图 1 1 6】

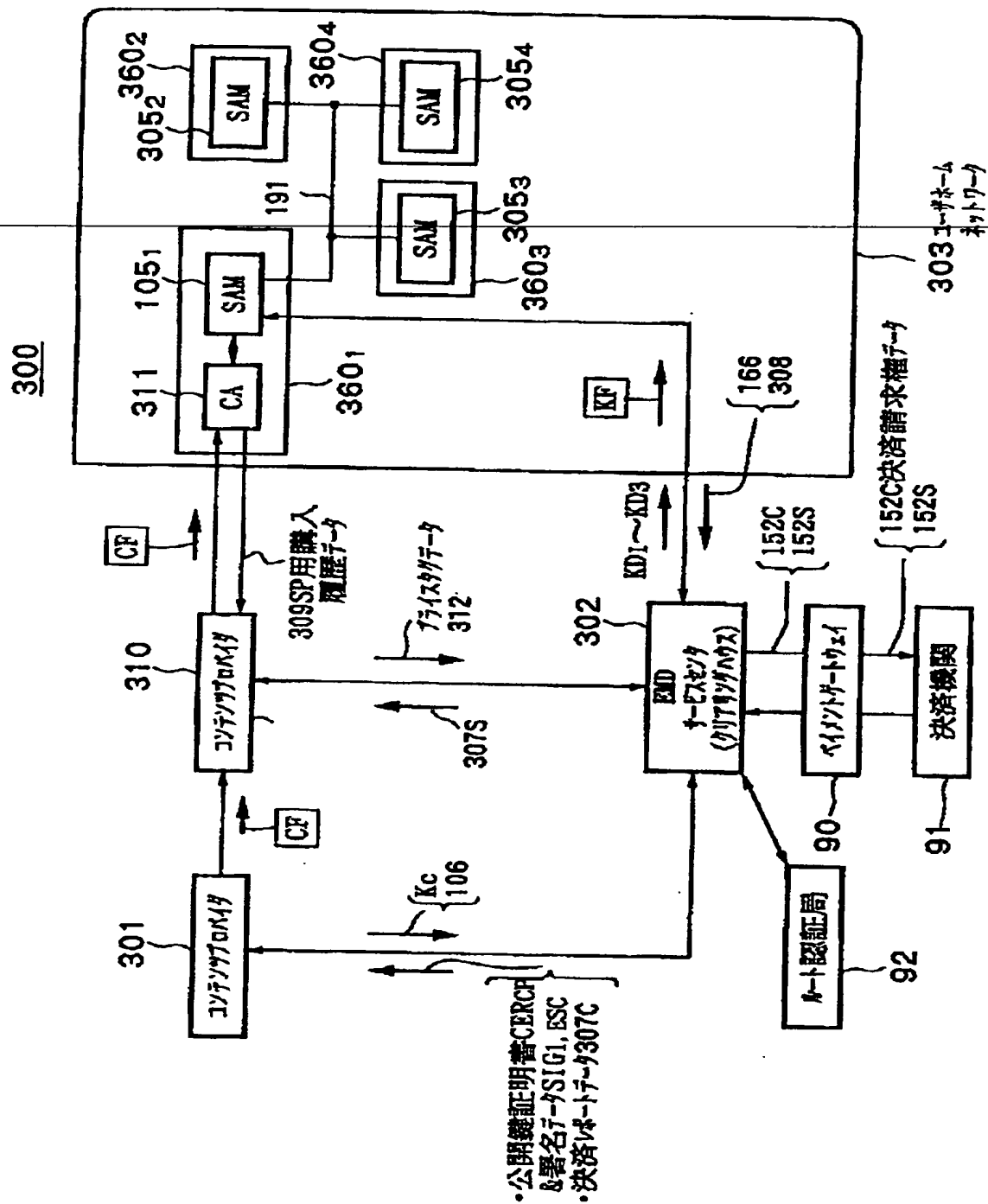
②-1-7-2-1-2 特殊インサート(インサート型)の加工方法-②

価格情報		署名	
署名	コピペ ID	署名	コピペ ID
署名	署名	署名	署名
署名	署名	署名	署名
署名	署名	署名	署名

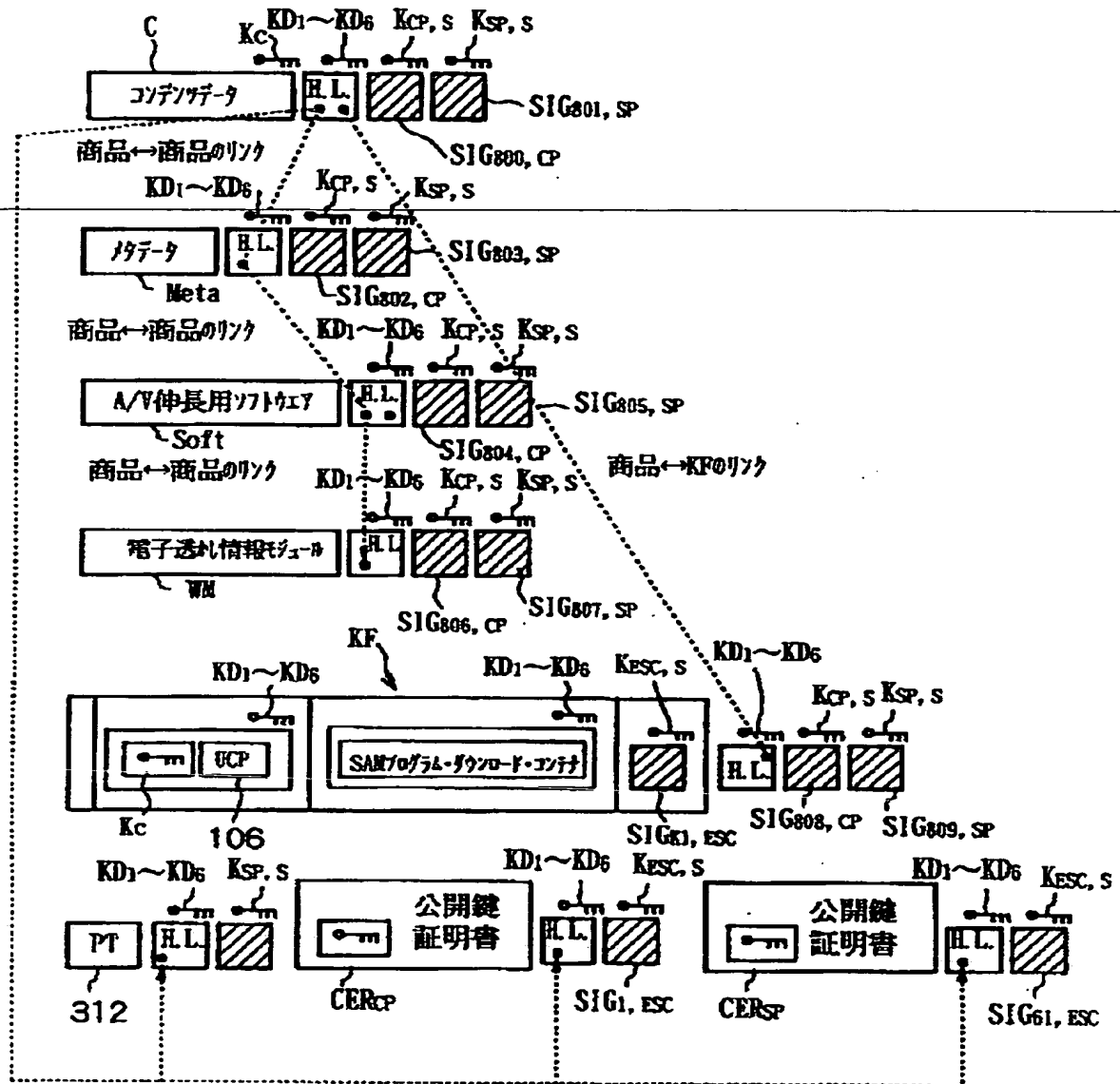
【図 1 1 7】



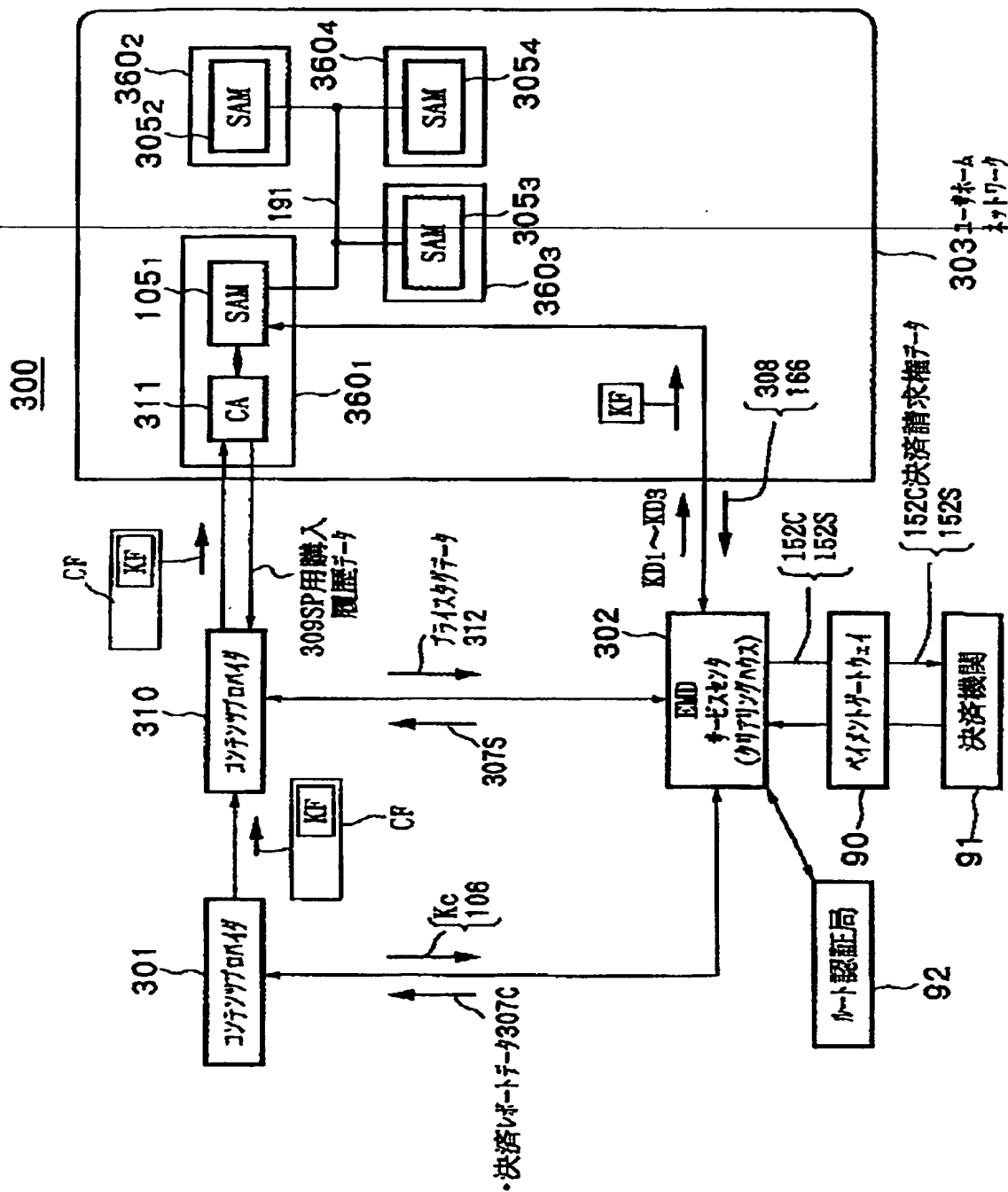
【図 1 1 8】



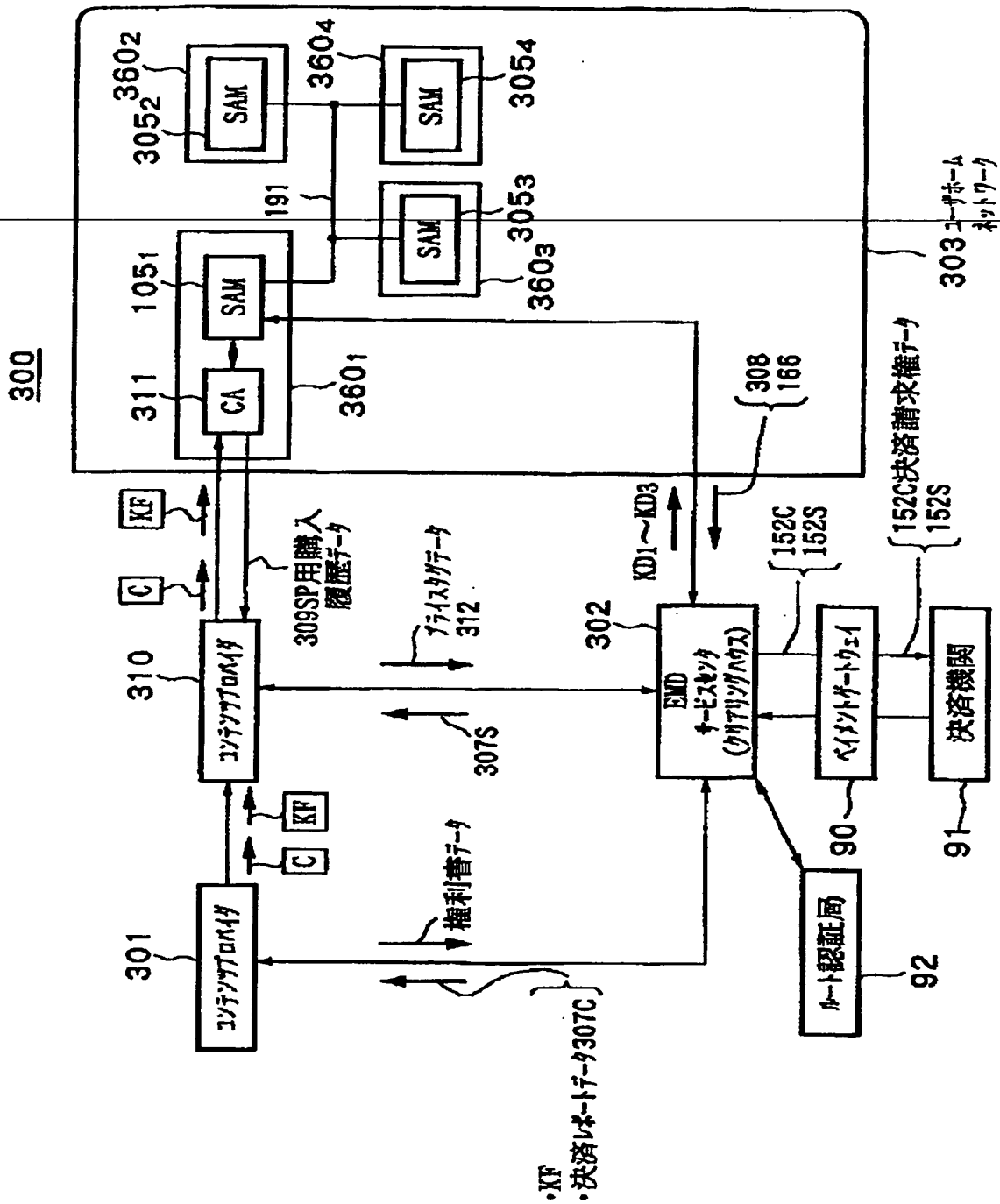
【図 119】



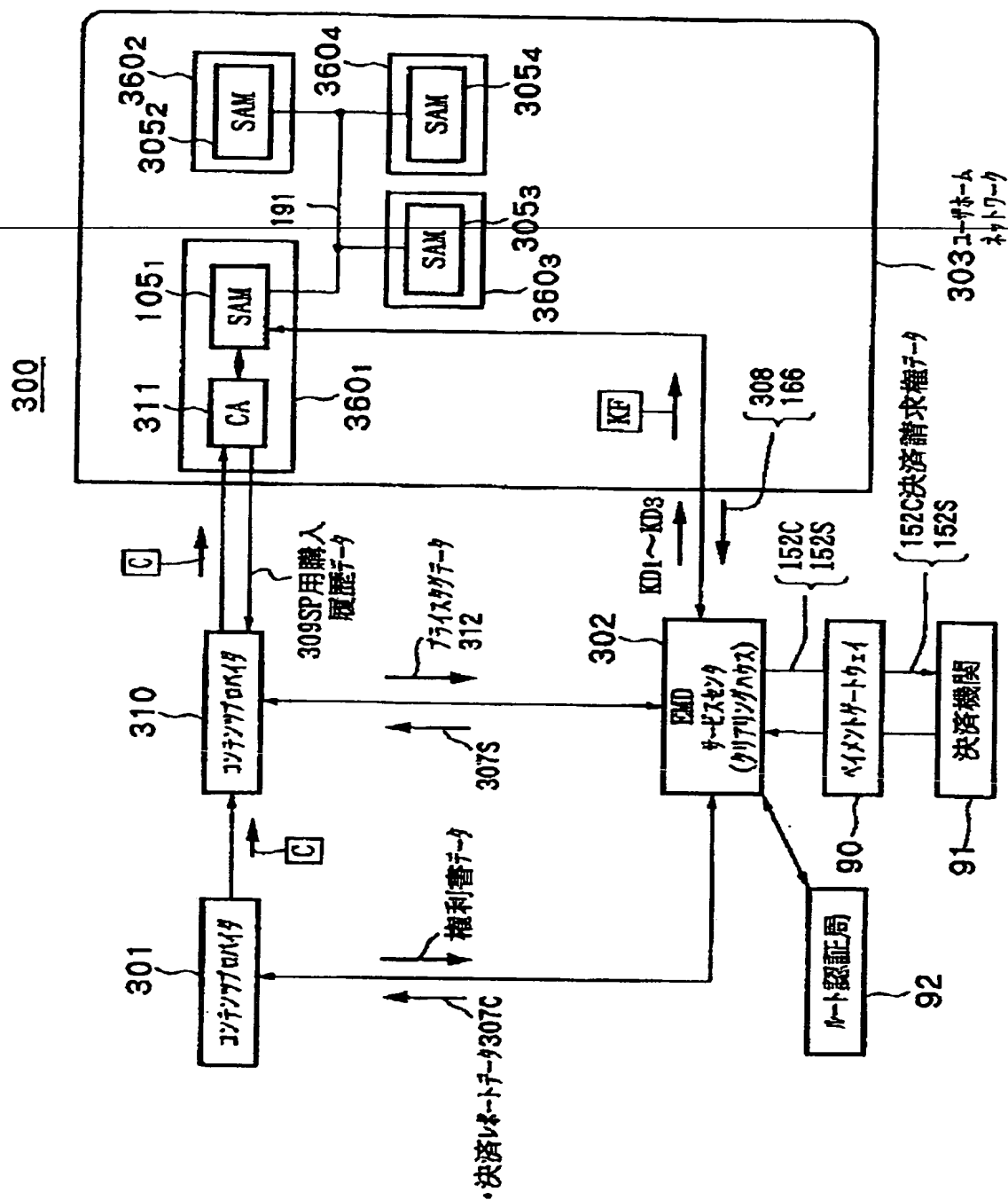
【図 120】



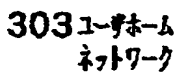
【図 122】



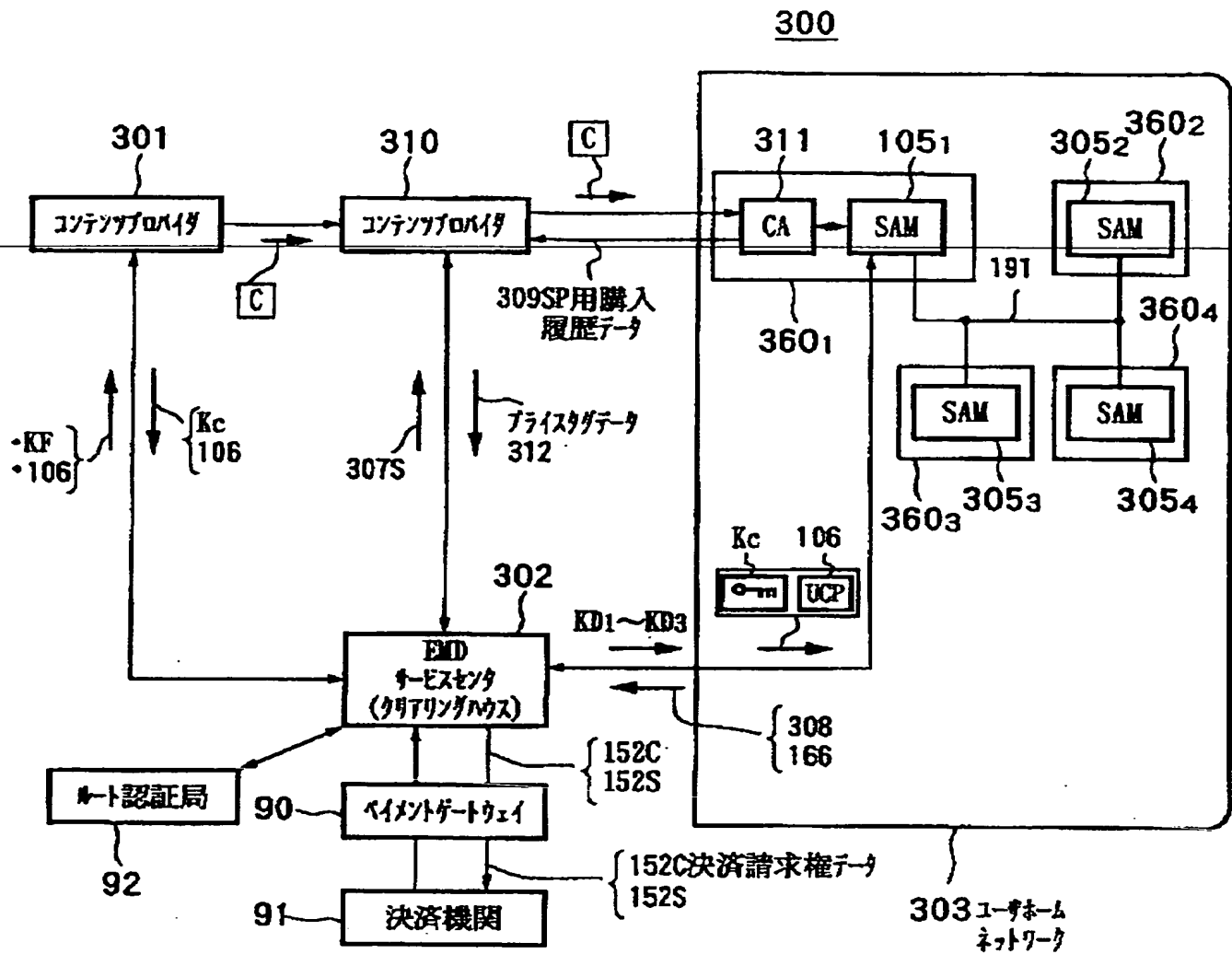
【図 1 2 3】



•KF
•106

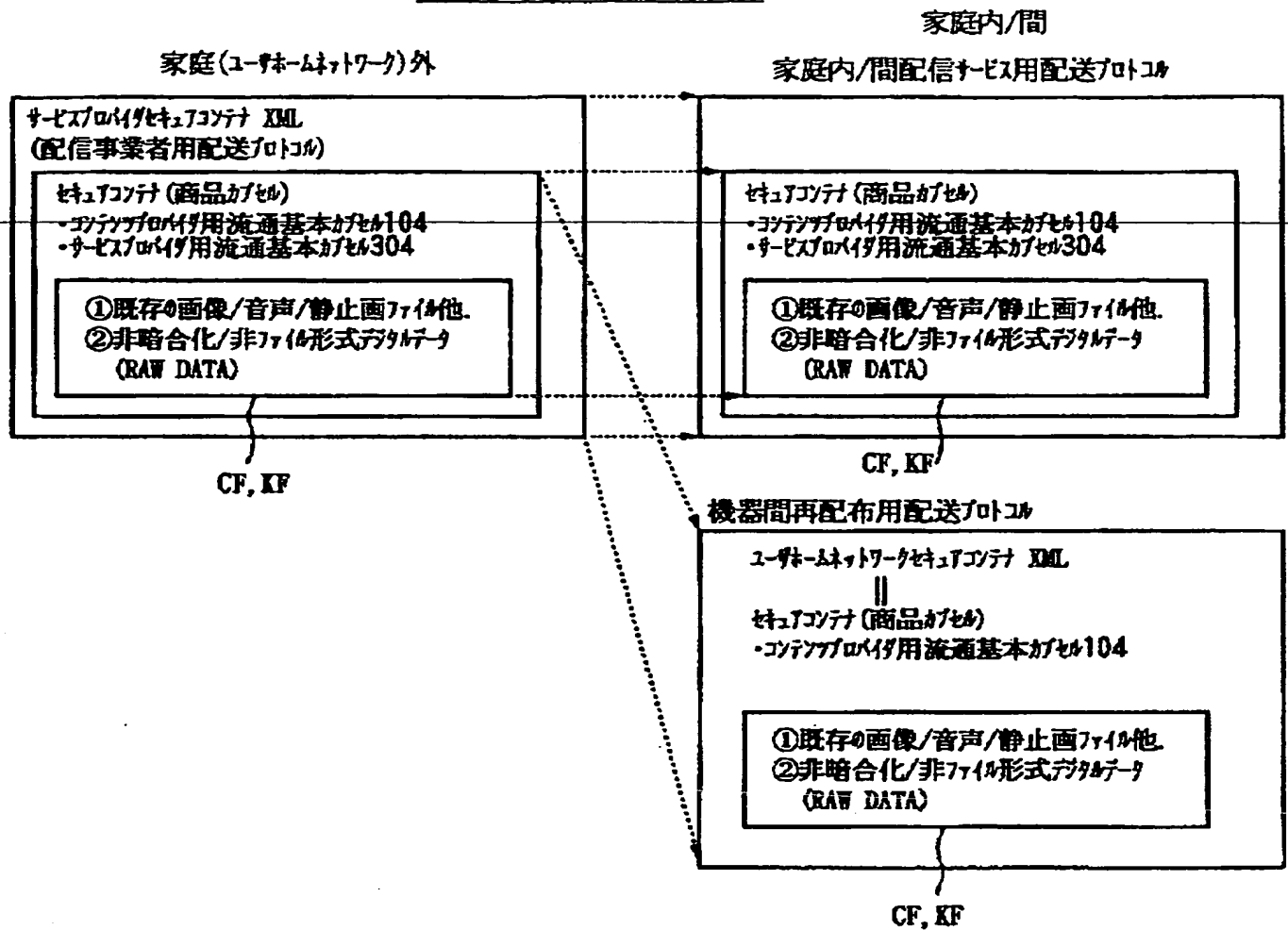


【図 125】

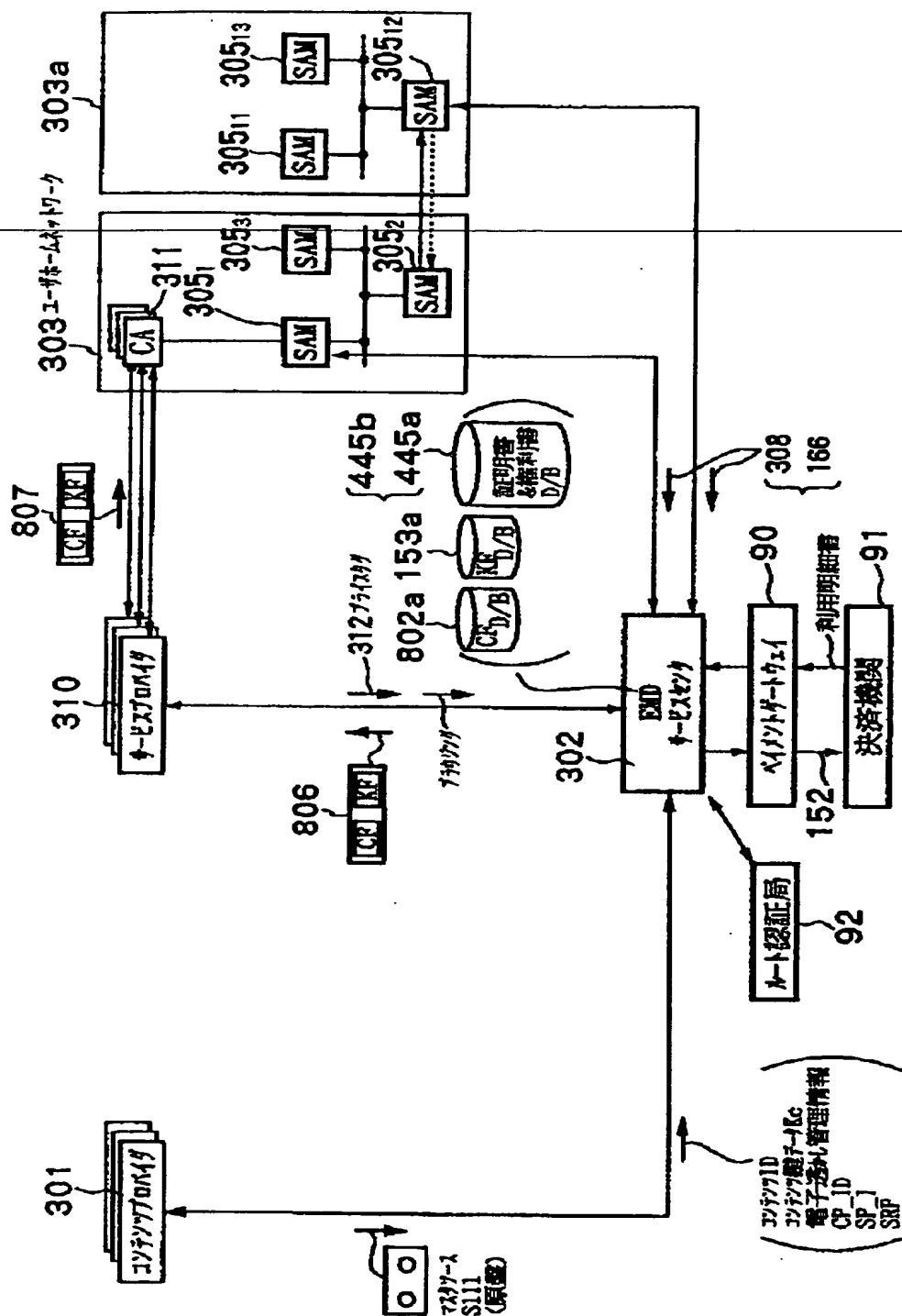


【図 127】

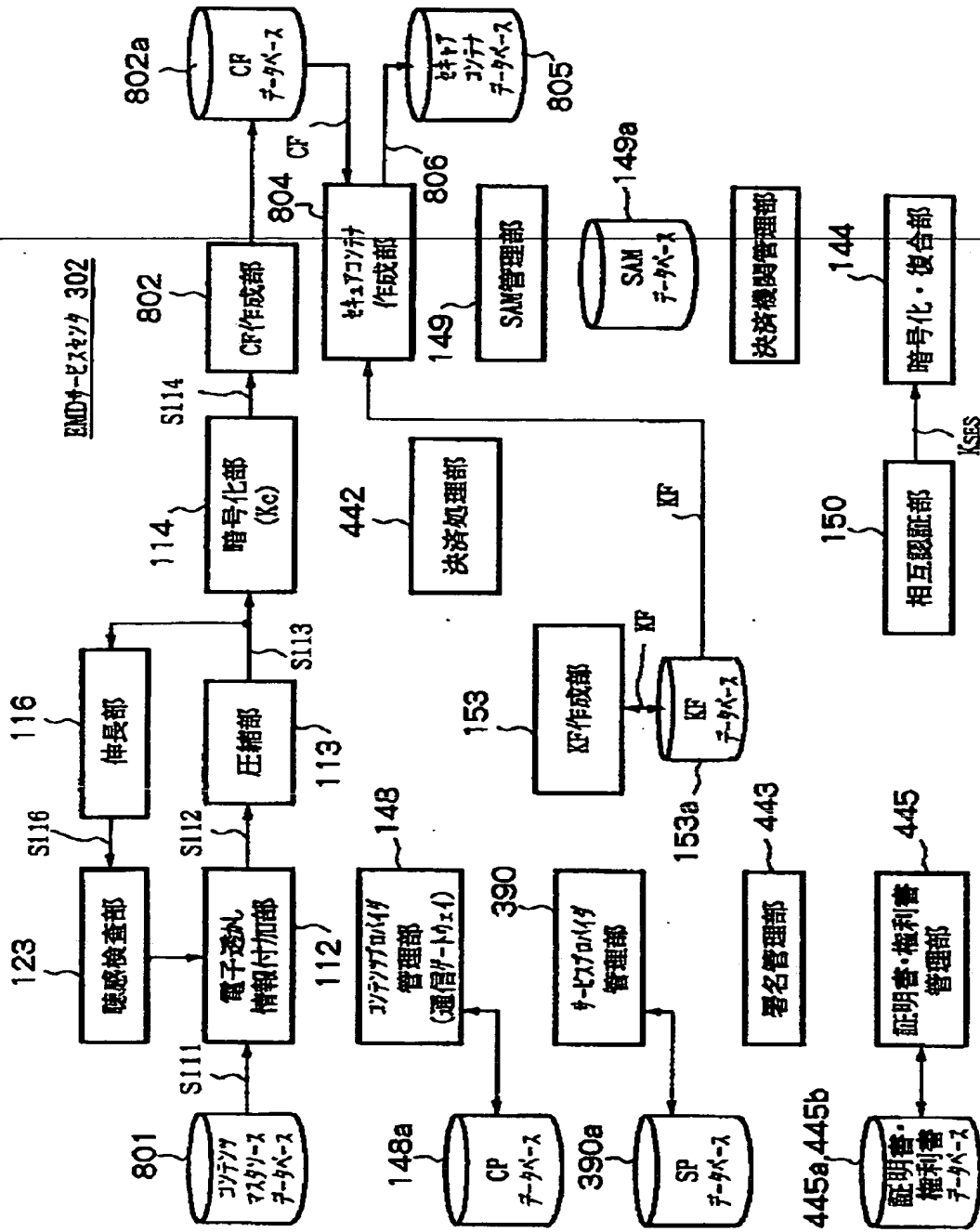
コンテンツのファイル包括大小関係



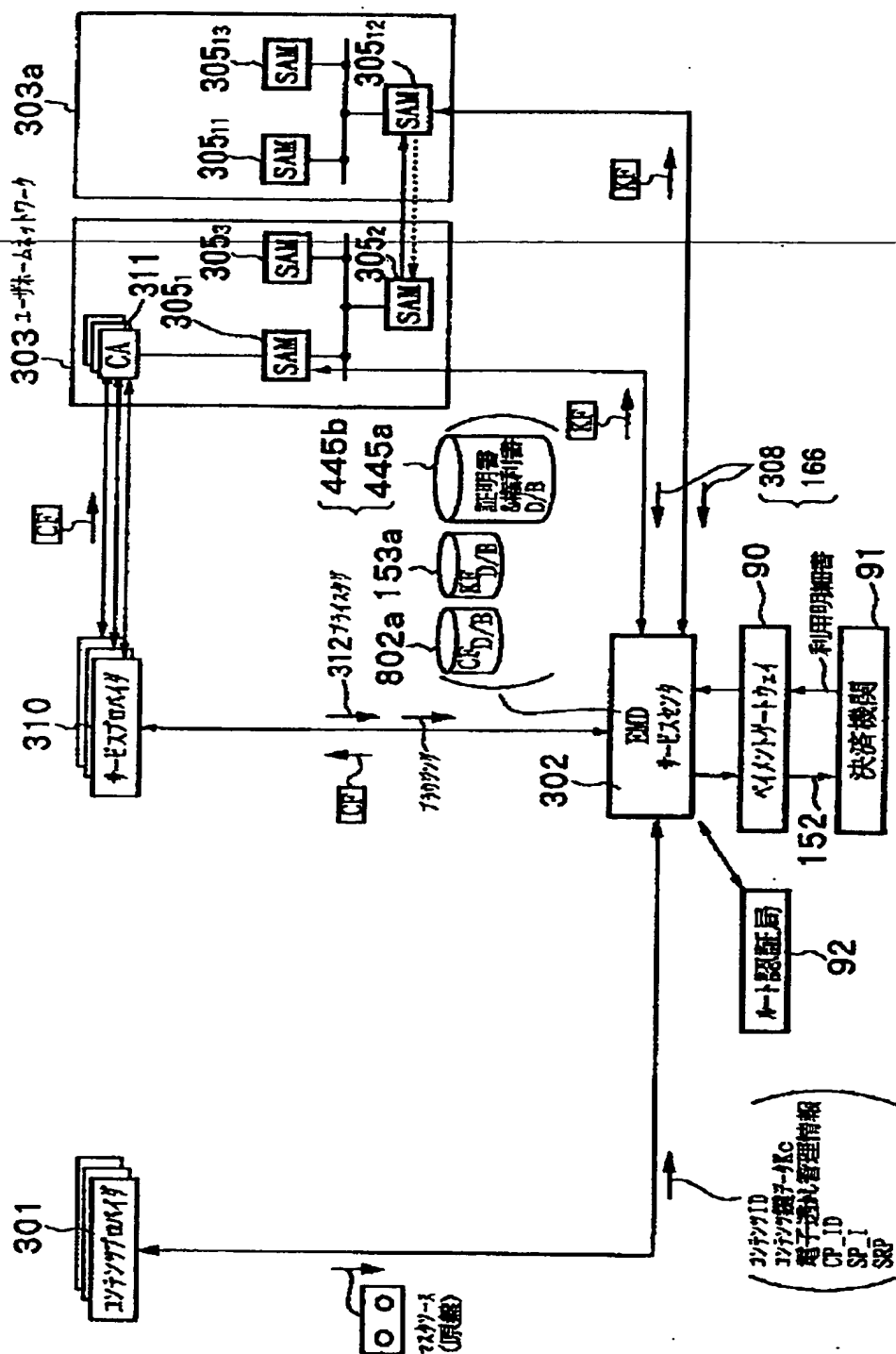
【図 1 2 8】



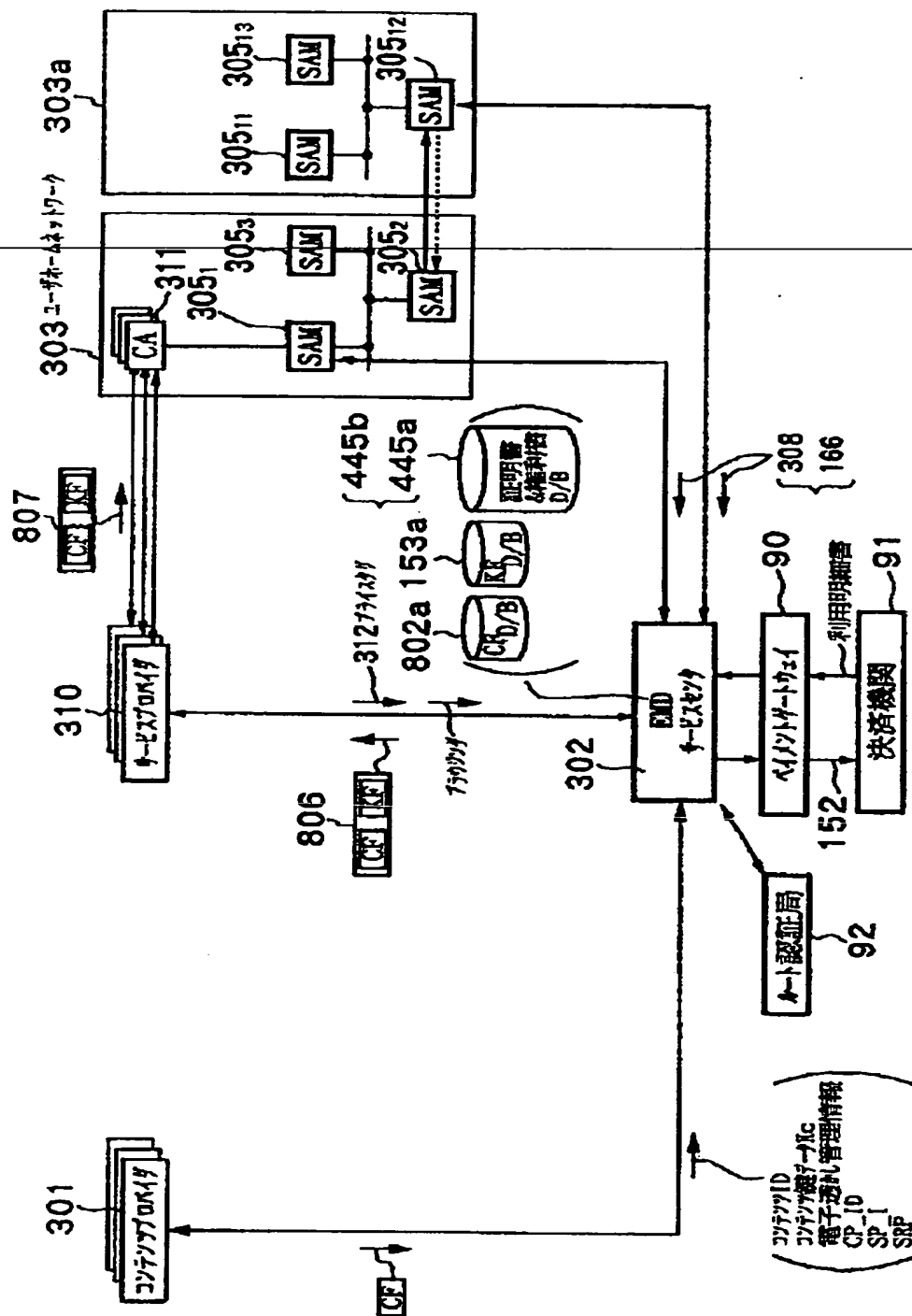
【図 129】



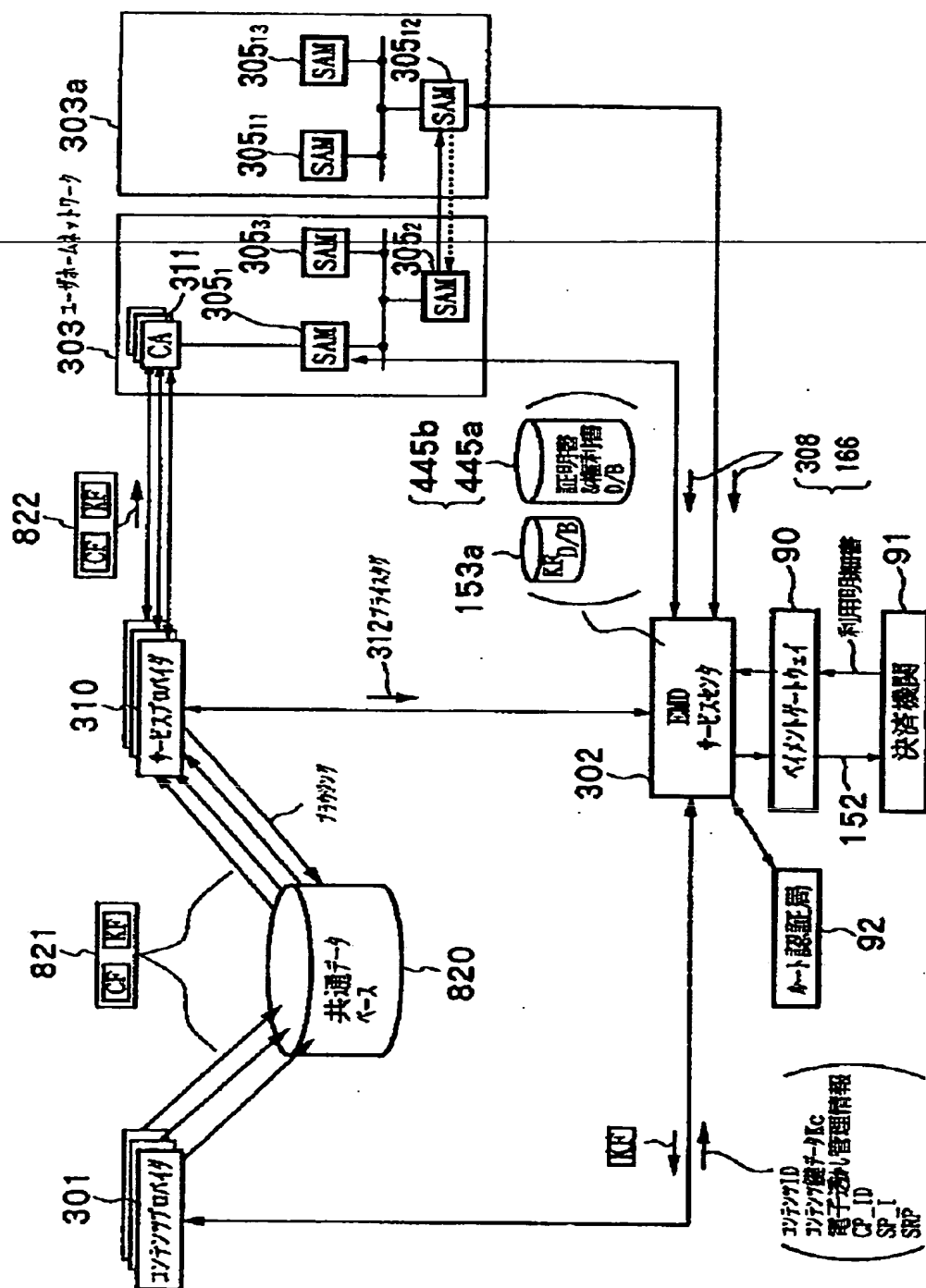
【图 130】



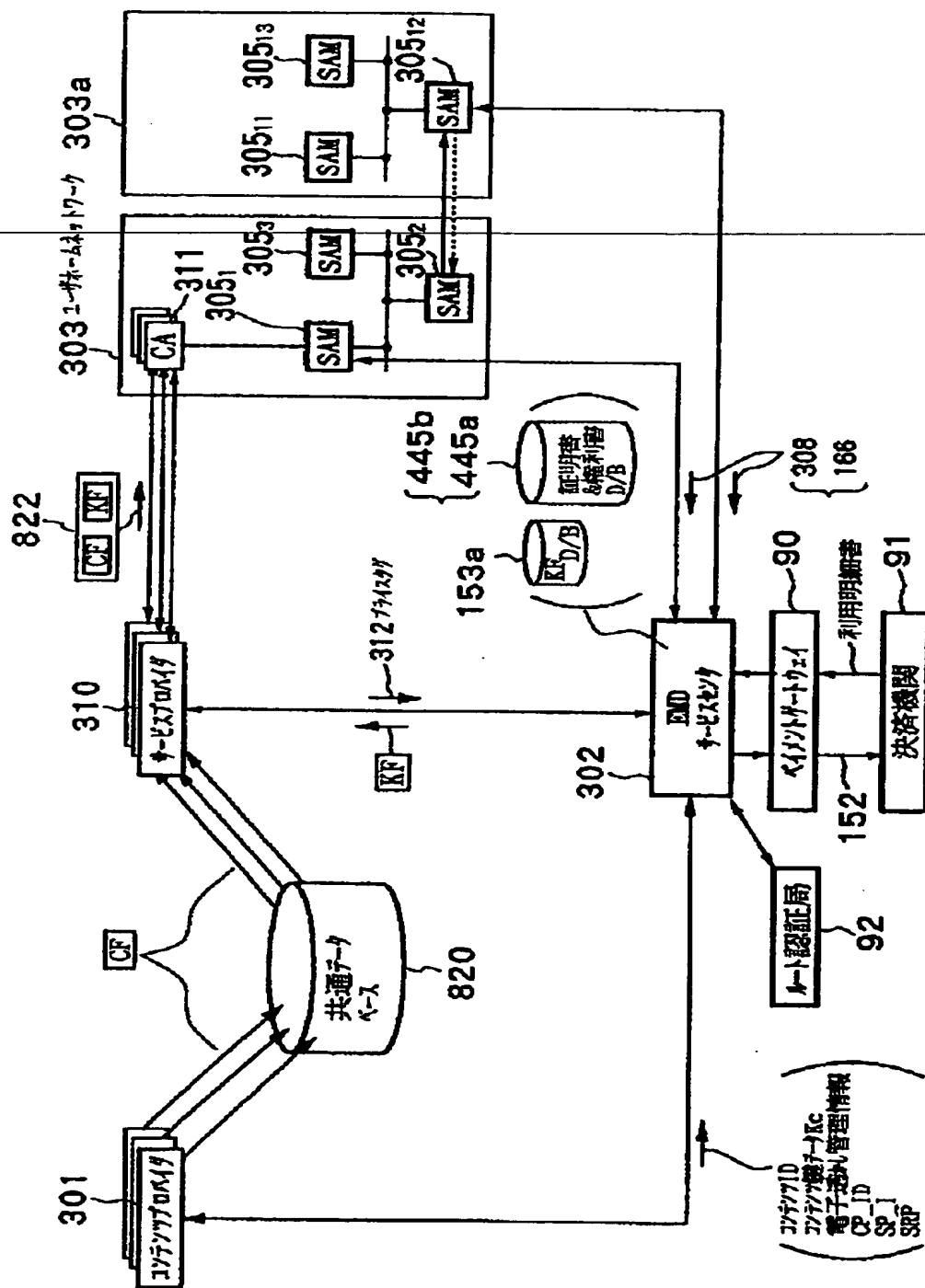
【図 1 3 1】



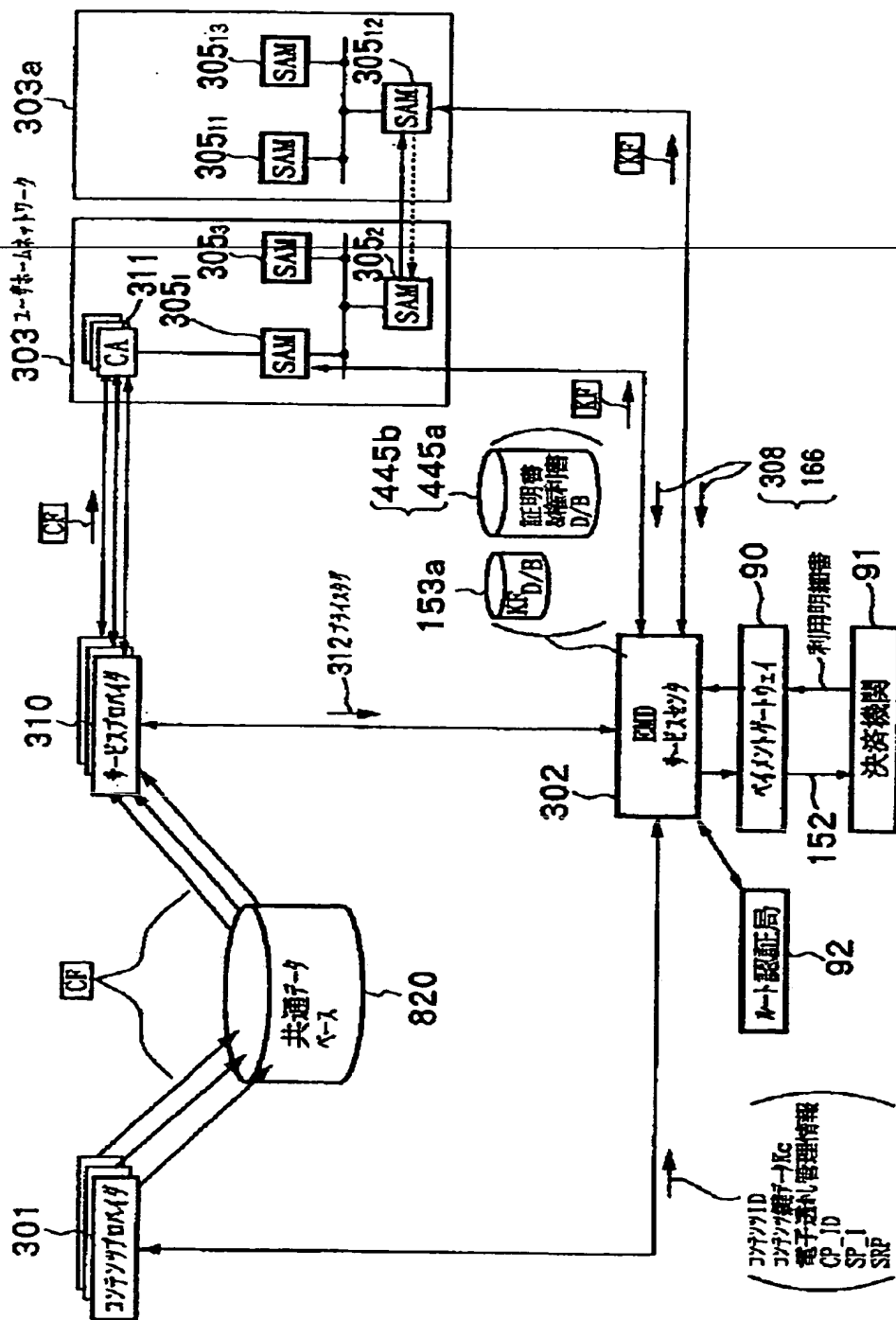
【図 1 3 3】



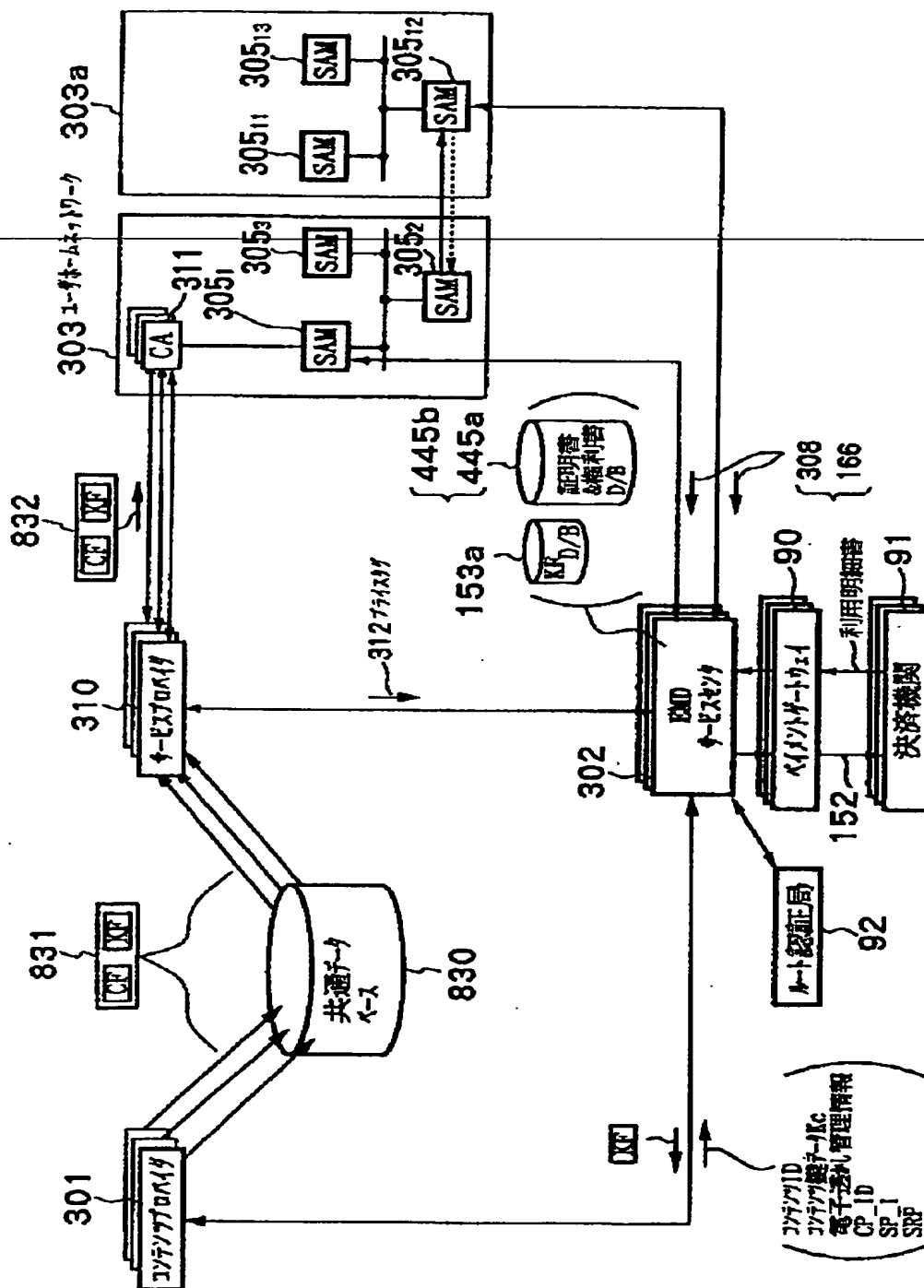
【图 1 3 4】



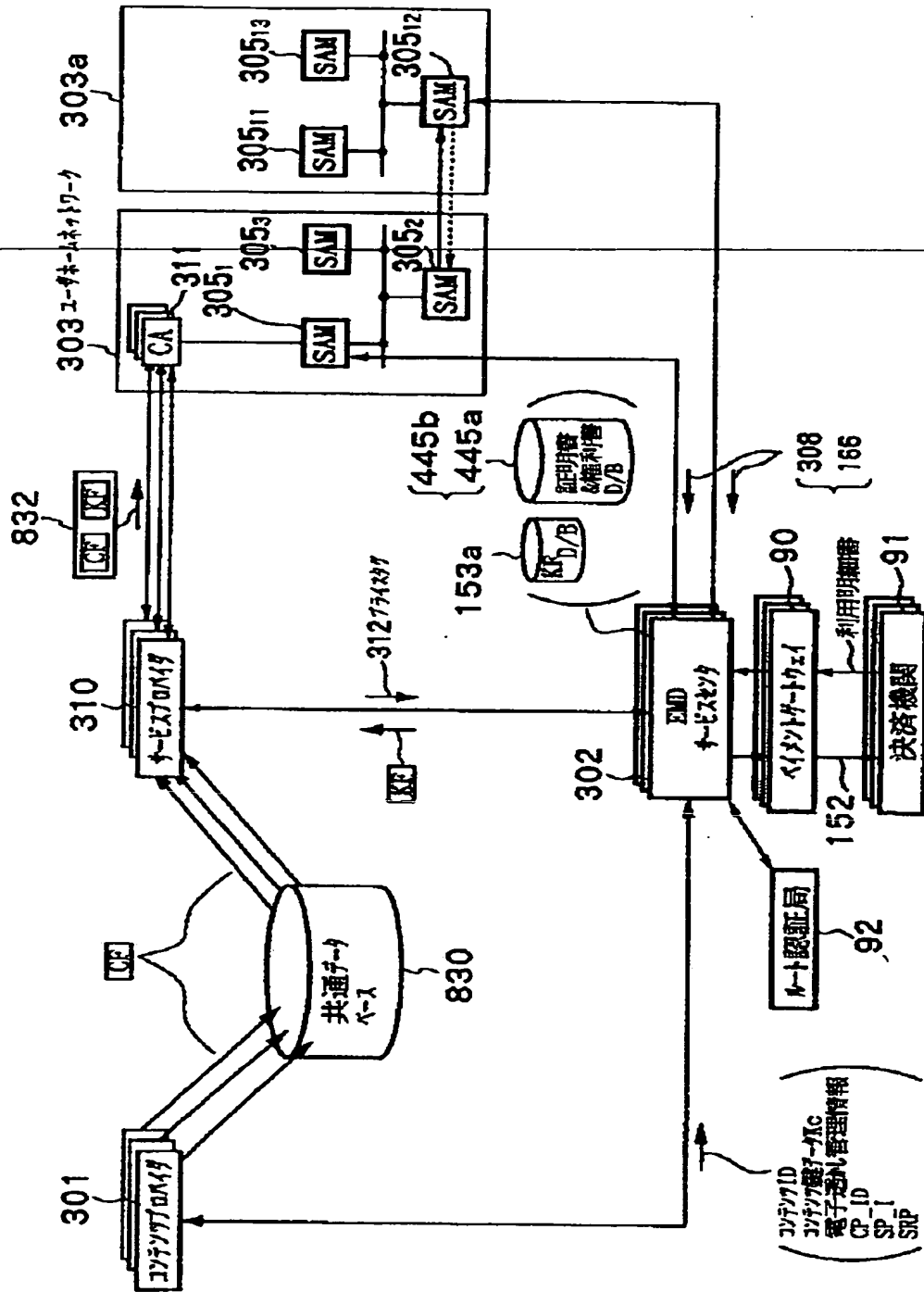
【図 1 3 5】



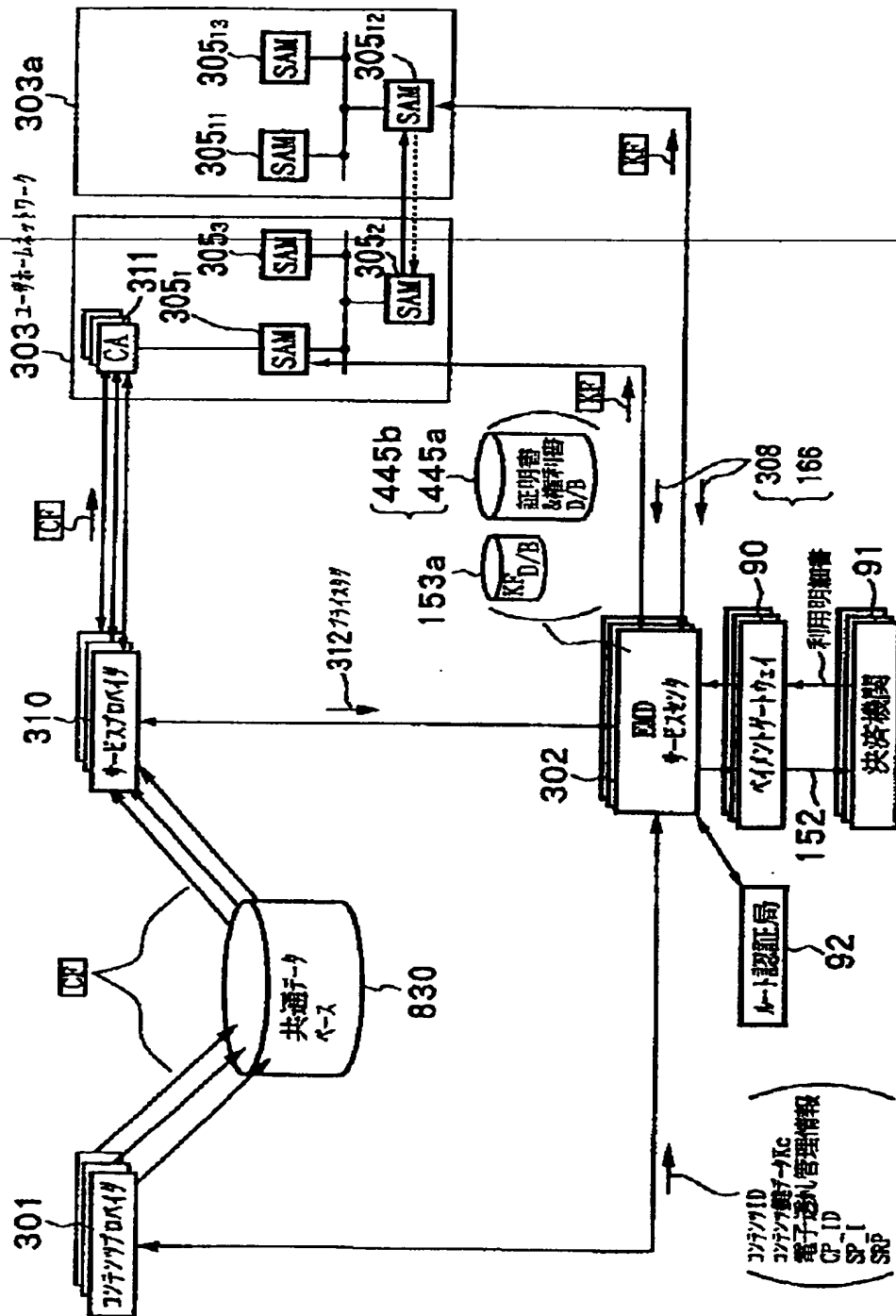
【図 136】



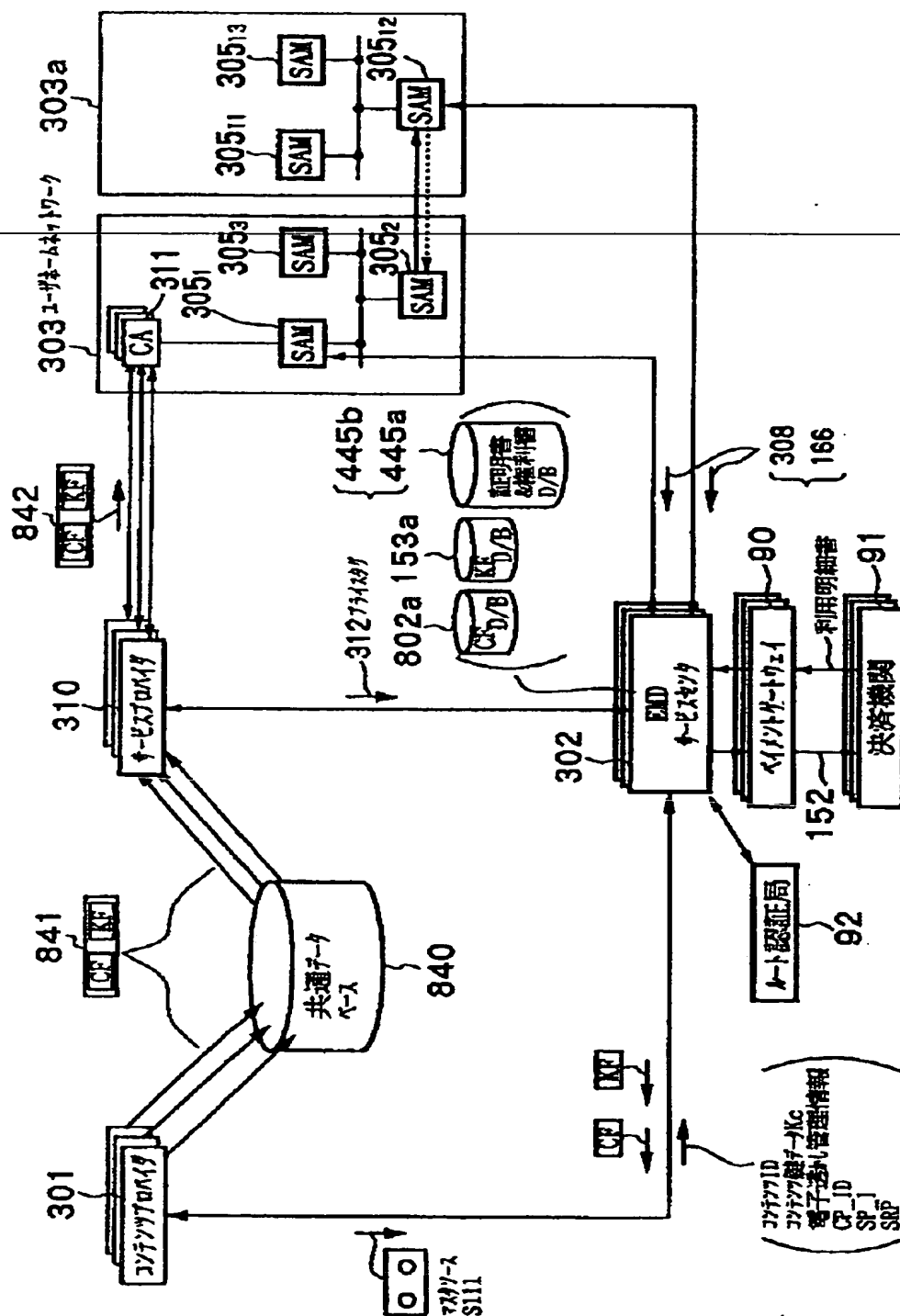
【図 137】



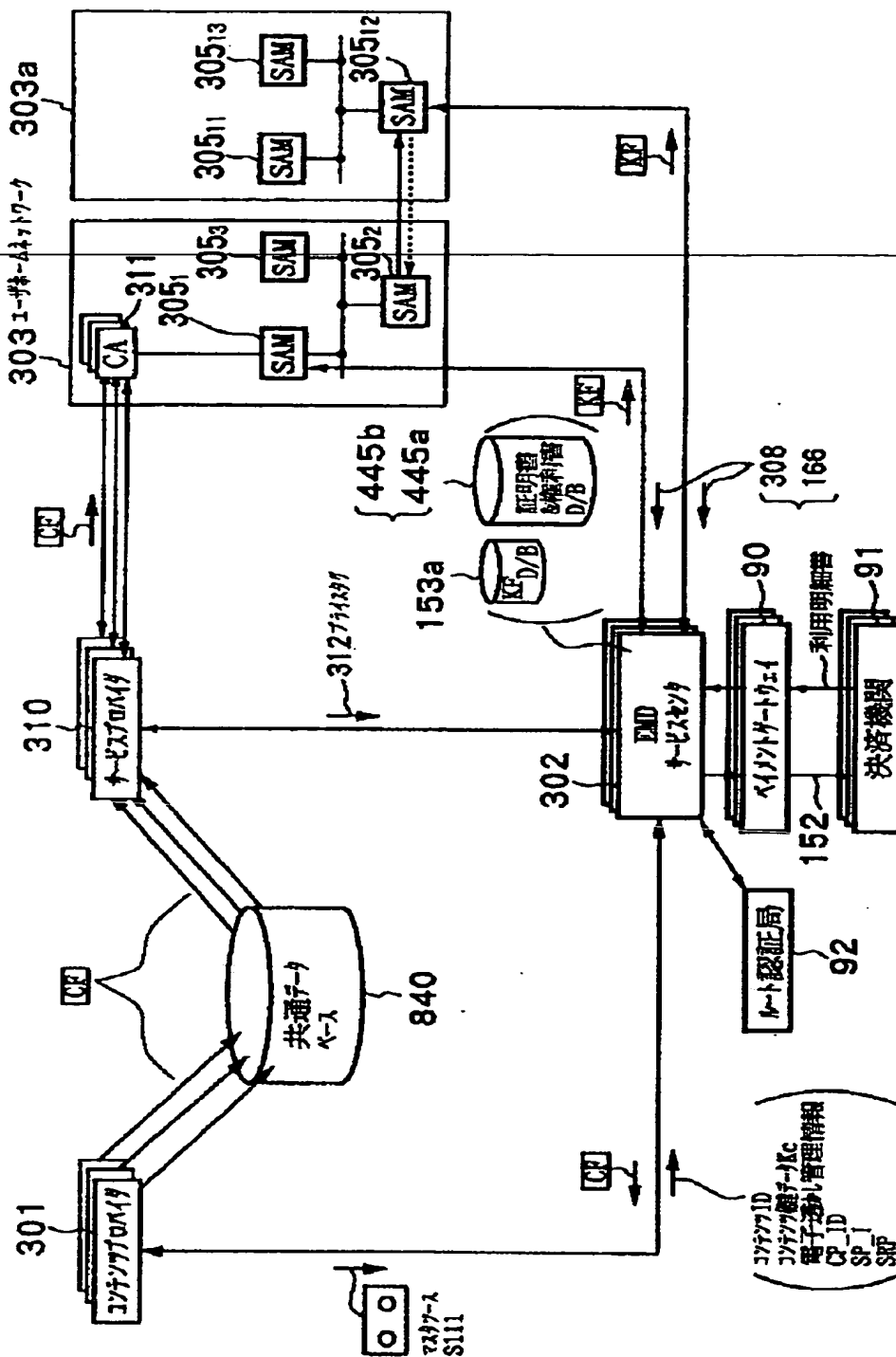
【図 1 3 8】



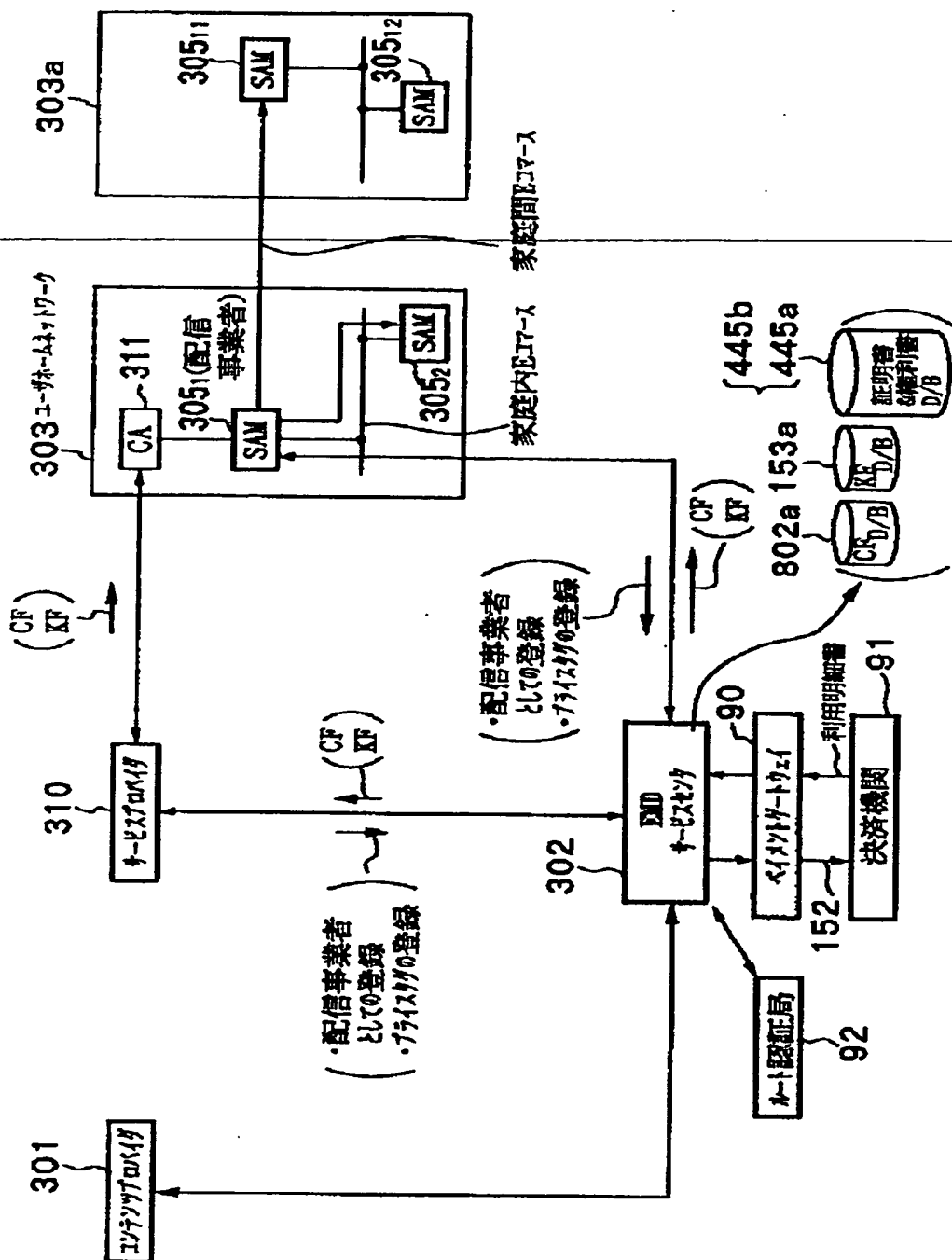
【图 1 3 9】



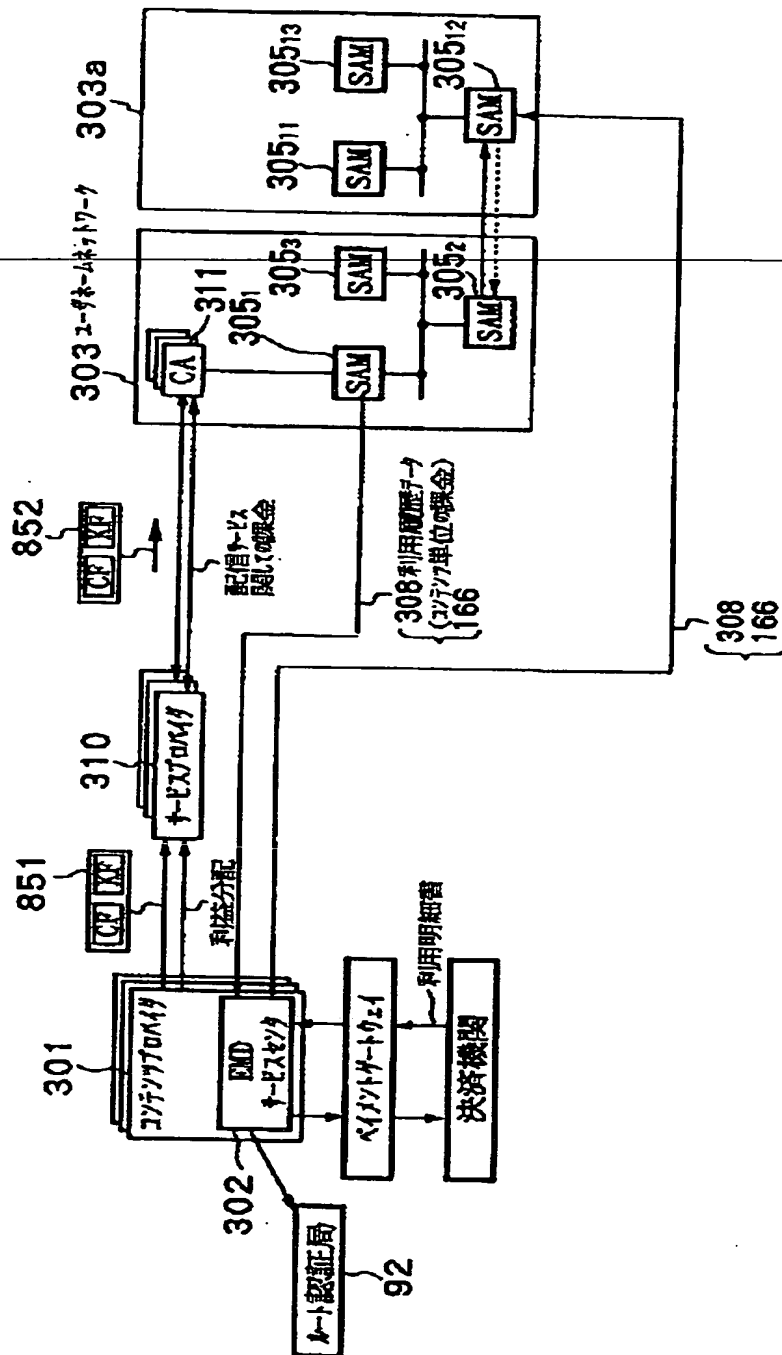
【図 1 4 1】



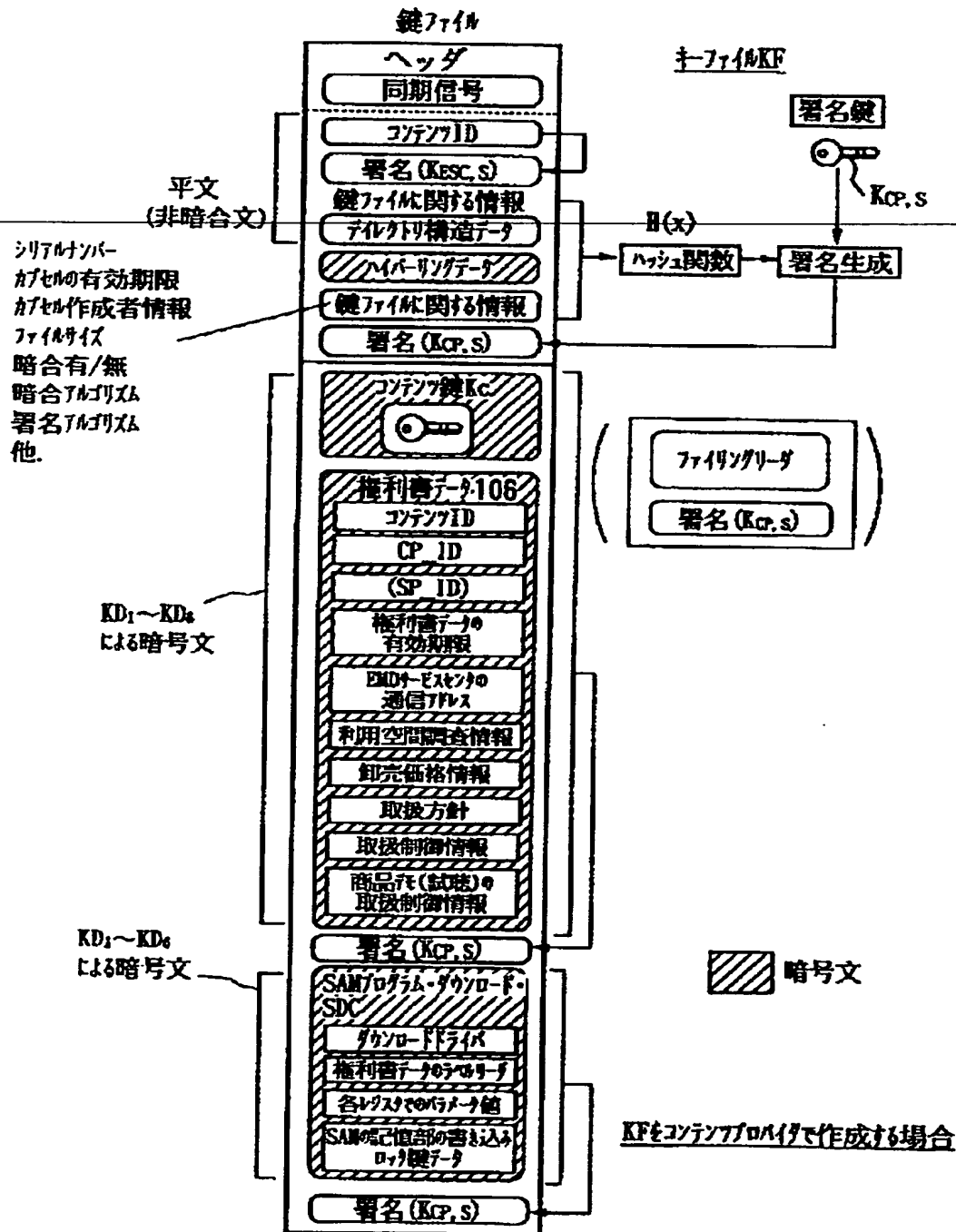
【図 1 4 2】



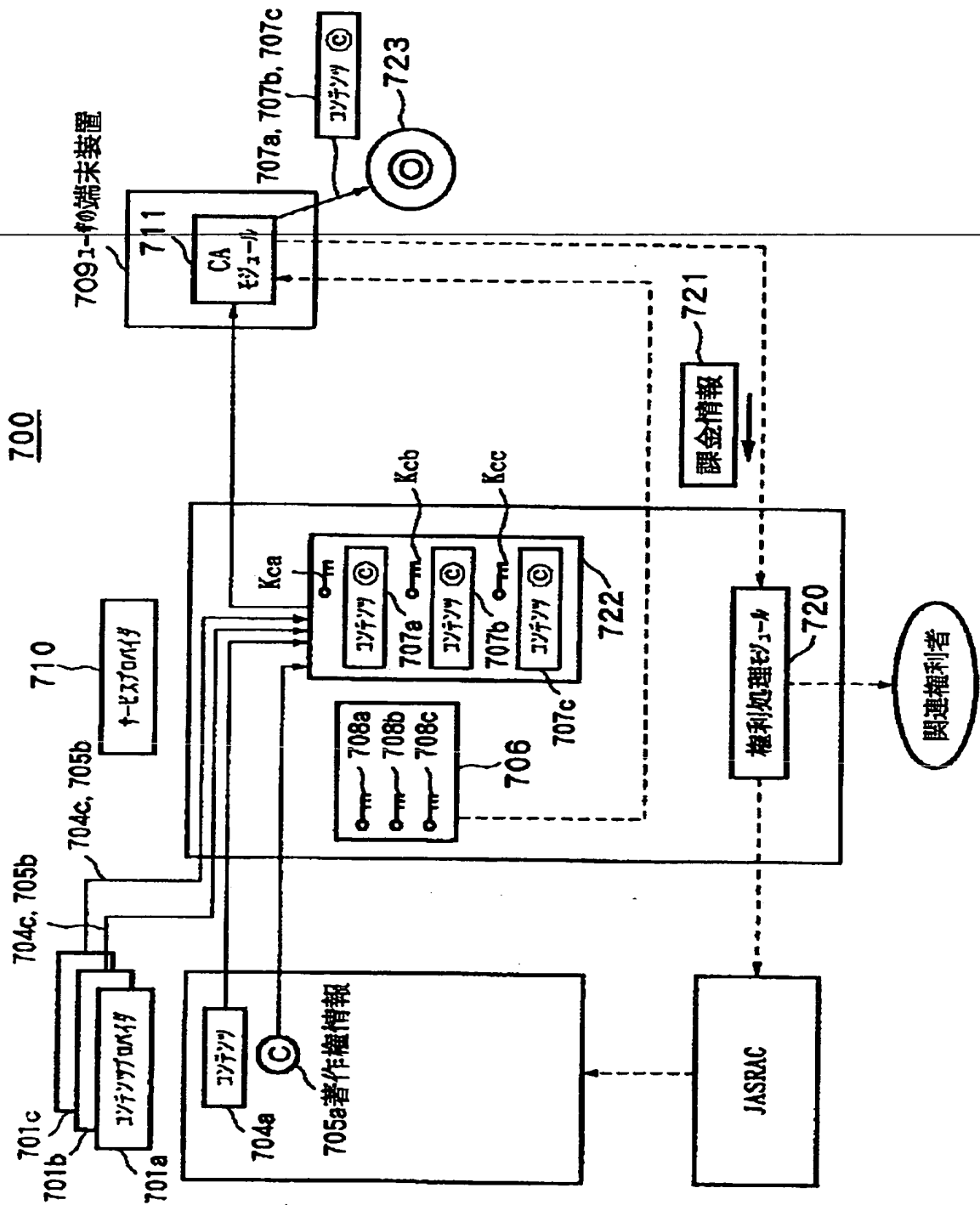
【図 143】



【図 144】



【図 1 4 5】



【書類名】 要約書

【要約】

【課題】 データ提供装置の関係者の利益を保護できるデータ提供システムを提供する。

【解決手段】 コンテンツプロバイダ 1 0 1 は、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、配信鍵用データを用いて暗号化されたコンテンツ鍵データと、コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したセキュアコンテナ 1 0 4 をユーザホームネットワーク 1 0 3 の S A M 1 0 5 ₁ などに配給する。S A M 1 0 5 ₁ などは、セキュアコンテナ 1 0 4 に格納されたコンテンツ鍵データおよび権利書データを復号し、当該復号した権利書データに基づいて、コンテンツデータの購入形態および利用形態などの取り扱いを決定する。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号

[000002185]

1. 変更年月日	1990年 8月30日
[変更理由]	新規登録
住 所	東京都品川区北品川6丁目7番35号
氏 名	ソニー株式会社

This Page Blank (uspto)